

LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH



Policy Title: Access to Integrated Behavioral Health Information System

Policy Number: 550.04

Policy Category: Administrative

Distribution Level: Directly-Operated Programs and Contracted Agencies

Responsible Party: Chief Information Office Bureau

I. POLICY STATEMENT

The purpose of this policy is to ensure the confidentiality, integrity, and availability of all information entered and maintained in Los Angeles County Department of Mental Health (DMH/Department) Integrated Behavioral Health Information System (IBHIS) using Avatar™ Electronic Health Record (EHR) System.

This policy outlines the acceptable use of DMH EHR System.

This policy informs all authorized workforce members of their responsibilities and accountability for the protection and confidentiality of clients' sensitive information viewed, maintained, and/or accessed using the DMH EHR System.

This policy outlines the establishment of authorized workforce member identities and obligation to protect their electronic signature when signing electronic documents and forms in IBHIS.

This objective of this policy is to maintain the confidentiality of Protected Health Information (PHI) and integrity of clinical records as required by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and other applicable federal, State, and local laws and regulations related to confidentiality by establishing a process for authorized workforce members to:

- Request a new IBHIS access account;
- Modify an existing account;
- Deactivate an account; and/or
- Reinstate a previously deactivated account.

Contracted agencies shall develop an internal policy and associated procedures that are consistent with their organizational practices and meet the requirements set forth in this policy.

II. DEFINITIONS

Terms used within this policy are defined in the DMH Information Technology and Security Glossary

LOS ANGELES COUNTY

DEPARTMENT OF MENTAL HEALTH



Policy Title: Access to Integrated Behavioral Health Information System

Policy Number: 550.04

III. POLICY

This policy applies to all the IBHIS users and outlines the processes for requesting, managing, and deactivating accounts, and establishes how monitoring and tracking shall take place within DMH. (DMH Policies 551.01 and 556.01).

This policy applies to all IBHIS DMH workforce members who have or are responsible for an account in DMH EHR System.

This policy also applies to IBHIS Non-DMH workforce members such as business associates, contracted employees, consultants, volunteers, other Los Angeles County departments and other non-employees who have a justified business need to access the DMH EHR System.

The IBHIS authorized workforce members should review the following DMH policies to ensure compliance with all policies related to inquiries and release of PHI and confidential data:

- DMH Policy 106.13, Reporting Possible Criminal Activity
- DMH Policy 500.01, Use and Disclosure of Protected Health Information Requiring Authorization
- DMH Policy 500.02, Uses and Disclosures of Protected Health Information Not Requiring an Authorization
- DMH Policy 500.03, Minimum Necessary Requirements for Using and Disclosing Protected Health Information
- DMH Policy 506.02, Privacy Sanctions
- DMH Policy 506.03, Responding to Breach of Protected Health Information
- DMH Policy 508.01, Safeguards for Protected Health Information
- DMH Policy 555.02, Information Technology and Security
- DMH Policy 551.01, Information Access Management
- DMH Policy 556.01, Acceptable Use for County Information Technology Resources
- DMH Policy 557.02, Appropriate Use of Email for Transmitting Protected Health Information and/or Confidential Data

Note: This is not necessarily a complete list of applicable policies.

All DMH policies and legal requirements (listed above) pertinent to confidentiality shall be maintained and observed.

DMH management shall cultivate and maintain a high level of employee awareness of the importance of data security. Employee awareness shall consist of a signed

LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH



Policy Title: Access to Integrated Behavioral Health Information System

Policy Number: 550.04

acknowledgement of responsibility under this policy and other security policies and procedures (listed above) that DMH has implemented.

IBHIS modules contain PHI, as defined by HIPAA, and as such, strict policies regarding the account usage and monitoring of accounts must be in place to prevent unauthorized access to the system. (DMH Policies 500.01, 500.02, and 500.03)

IBHIS Local User Administrators (IBHIS LUAs) and IBHIS Super Users shall create, activate, manage, and monitor the usage of unique individually named user accounts and inactivate accounts when access is no longer required.

Only authorized workforce members may access PHI or confidential data via IBHIS.

Note: DMH workforce members shall complete the DMH version of the above forms where the non-DMH workforce members shall submit the non-DMH version.

As the Avatar™ EHR System is a web-based application containing PHI, user accounts must be closely monitored and maintained to prevent unauthorized access. Avatar™ user reports shall be utilized to monitor appropriate access and use of this web-based system.

No workforce member shall allow any other individual to use his/her logon ID and password to access IBHIS.

Levels of access for any individual authorized to use the IBHIS shall be limited to the data necessary to carry out his/her specific assigned duties and responsibilities.

Distribution and use of reports containing PHI shall follow relevant DMH privacy policies and procedures to include clear labeling of each page as “Confidential Information.” (DMH Policy 500.01, 500.02, and 500.03)

Inquiry and/or release of client information must comply with all relevant DMH policies. (DMH Policies 500.01, 500.02, and 500.03)

No person may copy, export, download, store, save, print, print screen, photograph, or video-graph displayed information from IBHIS without prior written authorization from DMH Departmental Privacy Officer (DPO) and Information Security Officer (DISO) unless the action listed above is an approved part of conducting business as defined by the user’s role. All acquired information containing PHI, in paper or electronic format, must be stored, or transported by departmental approved methods in accordance with DMH Policy 508.01 and Security and Privacy Rule (45 CFR Parts 160 and 164).

Per DMH Policy 506.03, known or suspected security violation must be reported immediately to the workforce member’s supervisor.

LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH



Policy Title: Access to Integrated Behavioral Health Information System

Policy Number: 550.04

Facility and Program Heads are responsible and must take appropriate action when they become aware of a security violation concerning PHI by an IBHIS user at their facility (DMH Policy 506.02). Such action includes notification to DMH DISO or contacting Help Desk.

DMH shall ensure the systems and operating procedures developed and operated by and for DMH contain internal and external controls that there is no concentration of authority sufficient for one individual to commit undetected malicious or fraudulent acts.

All IBHIS DMH workforce members, whether permanent, temporary, or part-time, shall be held personally accountable for their actions or negligence in ensuring the confidentiality, integrity, and availability of IBHIS.

- DMH workforce members who violate this policy may be subject to appropriate disciplinary action up to and including discharge.

Note: Failure to comply with HIPAA can result in civil and criminal penalties (42 USC §1320d-5).

- Non-DMH workforce members with access to the IBHIS who violate this policy may be subject to termination of contractual agreements, denial of access to County Information Technology resources, and other actions including both civil and criminal penalties.

IV. PROCEDURES

[Click here to view procedures.](#)

V. AUTHORITIES

[Code of Federal Regulations Title 45 Part 160, General Administrative Requirements](#)
[Code of Federal Regulations Title 45 Part 164, Security and Privacy](#)
[Board of Supervisors Policy 6.101 - Use of County Information Assets](#)

VI. ATTACHMENTS

[Agreement for Acceptable Use and Confidentiality of County Information Assets](#)
[Annual Report of Performance Evaluation](#)
[Confidentiality Oath \(DMH Workforce Members\)](#)
[Confidentiality Oath \(Non-DMH Workforce Members\)](#)
[DMH Avatar™ User Security Agreement \(DMH Workforce Members\)](#)
[DMH Avatar™ User Security Agreement \(Non-DMH Workforce Members\)](#)

LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH



Policy Title: Access to Integrated Behavioral Health Information System
Policy Number: 550.04

[DMH Information Technology and Security Glossary](#)
[Electronic Signature Agreement \(DMH Workforce Members\)](#)
[Electronic Signature Agreement \(Non-DMH Workforce Members\)](#)
[IBHIS Access Request Form](#)

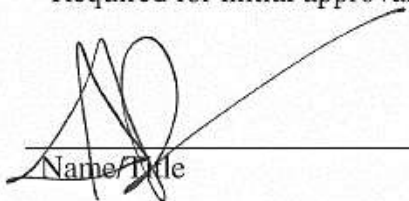
VII. EFFECTIVE DATES

This policy was effective January 20, 2015.

Review Date: May 21, 2019 Reviewed with Revisions

VIII. SIGNATURE, TITLE, and DATE OF APPROVAL

Required for initial approvals and all subsequent reviews and updates.



Name/Title

6-5-19

Date