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

COMPLIANCE, PRIVACY AND AUDIT SERVICES

PRIVACY OFFICE OPERATIONS HANDBOOK

LACDMH Privacy Office 2025

Table of Contents

FORWARD

At Los Angeles County Department of Mental Health (DMH), we recognize the vital importance of safeguarding the protected and confidential information of our consumers. As we navigate an increasingly complex digital landscape, we are committed to maintaining the highest standards of privacy and data protection. Our Privacy program is designed to ensure compliance with global data privacy laws, foster trust with those we service, and enable a secure environment where personal data is treated with the utmost respect.

The Privacy Office reflects the Department's dedication to proactive privacy practices, continuous monitoring, and the integration of privacy by design into every aspect of our operations. It is built on a foundation of transparency, accountability and a shared responsibility across all levels of our organization.

This handbook outlines the key elements of the Privacy program and the principles that guide our practices. DMH is committed to implementing policies and procedures that are aligned with Federal and State guidelines and regulations, ensuring the client's right to privacy of their mental health records.

We understand that privacy is not only a legal obligation but a core aspect of our reputation and relationship with our clients', stakeholders and community. As such, we are continually evaluating and enhancing our approach to privacy, striving to meet the evolving challenges the expectations of our clients, stakeholders, and partners.

Background

State and Federal privacy laws require DMH workforce members to protect clients' personal and medical information that we create and/or receive while providing services to our clients and as mental health authorities. Consequently, the DMH Compliance, Privacy and Audit Services (*CPAS*), Privacy Office establishes that all DMH workforce members are informed of their duties to protect clients' Protected Health Information (*PHI*) and Personally Identifiable Information (*PII*). Responsibilities of the Privacy Office include but are not limited to the following:

- Develop and implement privacy policies and procedures aligned with Federal and State guidelines.
- Train DMH workforce members on privacy policies and procedures.
- Conduct HIPAA compliancy reviews to ensure DMH workforce are in compliant with Federal and State privacy laws.
- Establish effective safeguards at mental health facilities and programs; and provide a process for workforce members to report violations of DMH privacy policies and breaches of PHI and PII.
- Investigate reported employee privacy violations/breaches to determine the validity of the allegations presented in the report.

PURPOSE

The intent of this handbook is to provide clear guidelines and protocols for handling personal and sensitive information within our organization. It serves as a comprehensive reference to support the Department's best practices, ethical standards and legal obligations when managing data. By following the guidelines and principles outlined in this handbook, Privacy ensures our organization maintains its commitment to data protection. Overview will be provided on:

- Key elements of HIPAA
- Federal and State Privacy Laws
- How to identify and report potential HIPAA violations and breaches
- Various privacy topics and how they relate to DMH's HIPAA privacy policies, including how to safeguard private and confidential information
- Other sensitive State and Federal privacy topics

KEY PRIVACY TOPICS

Privacy Laws

In addition to HIPAA, DMH must comply with other State and Federal privacy laws which provide extra protections to clients.

- Confidentiality of Medical Information Act (*CMIA*)
- Patient Access to Health Records Act (*PAHRA*)
- California Consumer Privacy Act (*CCPA*) – California Civil Code Section 5328
- California Privacy Rights Act (*CPRA*)
- California Data Breach Notification Law

Privacy Policies

DMH's HIPAA privacy policies and procedures (*Privacy policies No. s 500.01-510.01*). Both Privacy and Security Information policies and procedures can be located in the Department's Compliance Bridge Portal. Employees may access the portal at the following link: https://secure2.compliancebridge.com/lacdmh/portal

Privacy Practices Reminders

- It is workforce duty to protect PHI and PII.
- Only access PHI/PII you need to do your job.
- Do not use or disclose PHI or PII unless necessary for your job.
- Only provide the minimum amount of PHI or PII necessary.
- Follow all required safeguards.
- Dispose of PHI/PII properly according to DMH Policy No. 508.01.
- Use fax cover sheets and confidentiality statements.
- Do not leave unattended PHI/PII on desks or computers.
- Follow DMH password requirements, do not share or leave passwords where others might find them.
- Encrypt and properly secure computing devices.
- Save work containing PHI/PII on the network.
- Lock up mobile computing devices when not in use and transport in trunk of car between worksites.

- Never leave mobile computing devices unattended in public places.
- Encrypt e-mails containing PHI/PII when sending outside the County's secure network.
- Never open attachments from strangers.
- Immediately report suspected breaches or lost/stolen computer devices.
- Failure to follow DMH policies and procedures may lead to disciplinary action, including discharge, fines and penalties, and even prison.
- Even if you do not work in a clinic setting, or do not directly work with PHI or PII, you may encounter this information during your career with the County, so it is important to safeguard it.

Verification of Identity Prior to Disclosure of PHI

DMH must verify the identity and determine the authority of individuals requesting access to PHI, including clients, personal representatives, attorneys, and public officials.

Personal representatives may include parent, legal guardian, relative pursuant to a Caregiver's Authorization Affidavit, conservator, or person named in a health care power of attorney or advanced directive. Divisions/Programs must establish the level of workforce that can approve or grant access to PHI. Before workforce can be granted access, prior approval from the Program Manager, Administrative Deputy or Deputy Director is required.

For more information, refer to DMH Policy No. 500.06, Verification of Individuals Requesting Protected Health Information, and Policy 500.08, Use and Disclosures of PHI Requiring an Authorization from Legal or Personal Representatives.

Unauthorized Disclosures to the Media

In general, except in limited circumstances, affirmative reporting or disclosure to the media or the public at large about an identifiable patient, shall not be done without the client's knowledge and signed authorization. Disclosure of clients' PHI to the media without a signed authorization may result in disciplinary action.

Notice of Privacy Practices (NPP)

The HIPAA Privacy Rule requires DMH Divisions/Programs (with a direct treatment relationship to a client) provide them with the NPP no later than the date of first service delivery and make a good faith effort to obtain the client's written acknowledgment of receipt of the NPP. If the Division/Program maintains an office or other physical site where health care is provided directly to clients, the Division/Program must also post the NPP in the facility in a clear and prominent location where clients are likely to see it, as well as make the notice available to those who ask for a copy.

The purpose of the NPP is to inform clients how the covered entities, such as DMH, uses and discloses PHI. It informs clients about their rights and how the client may exercise their rights, including how the client may complain to DMH should they feel their rights have been violated.

A copy of the DMH NPP can be found on DMH's Internet website at https://dmh.lacounty.gov/our-services/consumer-and-family-affairs/privacy.

All DMH workforce members involved with direct patient care, or who have access to PHI, are required to read the NPP to ensure they are aware of the principles of HIPAA.

For more information, refer to DMH Policy No. 502.01, Notice of Privacy Practices.

Workforces are responsible for familiarizing themselves with the Department's Code of Organizational Conduct, Ethics and Compliance (*CCEC*), as it is a critical element of the DMH Compliance Program and sets the expectations for all Department staff.

HEALTH INSURANCE AND PORTABILITY AND ACCOUNTABILITY ACT (*HIPAA*)

HIPAA Defined

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. The primary goal of HIPAA is to make it easier for clients to keep health insurance, protect the confidentiality and security of healthcare information, and help the healthcare industry control administrative costs (*45 CFR Parts 160 and 164*).

HIPAA applies to covered entities, which are organizations that routinely handle PHI. HIPAA defines covered entities as health plans, health care clearing houses, and health care providers who electronically transmit health information in connection with transactions concerning billing and payment for services or insurance coverage. For example, hospitals, academic medical centers, physicians, and other health care providers who transmit information relating to claims transaction directly or through an intermediary electronically to a health plan are covered entities.

PHI is any information in the medical record or designated record set that can be used to identify a client. PHI is typically created, used, or disclosed while providing a health care service such as diagnosis or treatment. PHI can be in any form or media, whether electronic, paper, or oral. Individually identifiable health information is information including demographic information.

The following 18 identifiers are considered PHI, or individually identifiable information, and are protected by HIPAA:

- Names
- Geographic subdivisions smaller than a state (*street address, city, county, precinct, sometimes zip code*)
- All elements of dates (*birth date, admission date, discharge date, date of death, all ages over 89*).
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social Security numbers (*SSN*)
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers

- Vehicle identifiers and serial numbers *(including license plate numbers*)
- Devise identifiers and serial numbers
- Web Universal Resource Locators (*URLs*)
- Internal Protocol (*IP*) Address numbers
- Biometric identifiers, including finger/voice prints
- Full face photographic images and any comparable images; and
- Any other unique identifying numbers, characteristic or code, except for a code or other means of re-identification

HIPAA Requirements

HIPAA requires that covered entities such as DMH:

- Provide its Notice of Privacy Practices (*NPP*) to their clients.
- Develop policies, procedures, and safeguards to protect patient privacy, and provide clients with the ability to access and amend their records.
- Train workforce members on these policies and procedures.
- Safeguard patient records that contain PHI and other confidential records from unauthorized individuals.
- Account for specified disclosures of PHI.
- Establish a complaint mechanism for privacy concerns.
- Establish and enforce a system of sanctions for workforce members who violate privacy and security policies and procedures.
- Establish written agreements with business associates.
- Notify clients, the U.S. Department of Health & Human Services' Office for Civil Rights (*OCR*), and sometimes the media, in the event of a breach of PHI.

Clients' Rights Under HIPAA

Under Federal and State laws, clients can:

- Obtain an NPP from a provider explaining how it will use and disclose their information (*DMH Policy No. 502.01, Notice of Privacy Practices*).
- Access their records, and request copies and/or amendments (*DMH Policies 501.01, Client's Right to Access Protected Health Information and Confidential Data, and 501.06, Client Rights to Amend Mental Health Information*).
- Request that certain information be restricted from use or disclosure for Treatment, Payment, and Operations purposes (*DMH Policy No. 501.07, Client Right to Request Restrictions to Use and Disclosure*).
- Obtain an accounting of how their information has been disclosed for non-Treatment, Payment, and Operations purposes (*DMH Policy No. 501.03, Accounting of Disclosures of Protected Health Information*).
- Request that information be communicated in particular ways to ensure confidentiality (*DMH Policy No. 501.04, Client Rights to Request Confidential Communications of Protected Health Information*).
- Complain if they feel that we have used or disclosed their health information inappropriately (*DMH Policy No. 504.01, HIPAA Privacy Complaints*)
- Be notified of breaches to the extent required by law (*DMH Policy No.506.03, Responding to Breach of Protected Health Information*).

HIPAA Privacy Rule

The Privacy Rule establishes national standards for PHI. It applies to healthcare providers, health plans, healthcare clearinghouses, and business associates. This rule outlines the clients' rights to access, amend, and request restrictions on the use of their PHI. Defines the permitted uses and disclosures of client PHI/PII, specifying how and when it can be used. The rule also requires that clients provide authorization for uses and disclosures of their PHI when it is not related to treatment, payment, or healthcare operations.

HIPAA Security Rule

The Security Rule sets standards that safeguard the electronic PHI of clients. This rule applies to entities that create, receive, maintain, or transmit ePHI. There are three main safeguards that are necessary to maintain confidentiality of patient ePHI: administrative (training, risk assessments, and workforce management), physical (documents are locked away and screens are locked when not in use), and technical (encryption, access controls, and audit logs).

HIPAA Breach Notification Rule

Requires covered entities to notify impacted clients within 60 days of discovering a breach. The notification must include a description of the breach, the type of information involved, steps taken to mitigate the breach, and contact information for further inquiries. If a breach affects more than 500 clients, the State Department Health and Human Services-Office for Civil Rights must be notified along with local media outlets and a substitute notice placed on the covered entities website.

REPORTING A HIPAA BREACH

Definition of a Breach

A breach is “the unauthorized acquisition, access, use or disclosure of PHI/PII which compromises the privacy, security, or integrity of such information.”

Examples:

- Phishing, malware or ransomware that has resulted in the infiltration of clients’ PHI/PII.
- PHI/PII posted on social media outlets
- PHI/PII mailed to the wrong address or person.
- Loss or theft of paper documents containing PHI/PII.
- Loss or theft of an unencrypted laptop, flash drive, or other form of portable media containing PHI/PII.
- Paper containing PHI/PII that is not shredded before disposal.
- Accessing the PHI/PII of others who do not have a need to know and without the client’s signed authorization.

Suspected Breach

If workforce suspects a breach may have occurred, consult with a supervisor or program manager or contact the Privacy Officer directly for consultation.

Reporting a Suspected Breach

Complete the Privacy Incident Report and submit to the Privacy Office by the end of the business day via email address (Attachment A): Privacy@dmh.lacounty.gov

Workforce may also contact the Privacy Office directly to consult regarding the validity and/or what warrants a report.

Submitting a Privacy Incident Report

The Privacy Office staff will review the submitted report to determine if the privacy incident has resulted in a privacy violation or breach, logs the report into the Privacy Comprehensive Log for tracking and forward to the Privacy Officer for handling.

What happens if an incident is a reportable HIPAA Breach?

Upon reviewing the privacy incident report and determining a breach has occurred, the Privacy Office investigates and interviews all parties involved in the incident to determine the validity of the information provided and proceeds according to the HIPAA Breach Notification Rule, DMH policies and procedures for handling breaches and department protocols. (r*efer to DMH Policy No. 506.03, Responding to Breach of Protected Health Information*). If applicable, a HIPAA Complaint Investigative Report is submitted to DMH Human Resources Performance Management Unit (*PMU*) for further disciplinary determination.(Attachment B)

Reporting a Security Breach

If the breach involves electronic PHI/PII, due to a county or personal computer has been suspected of being compromised by a phishing, ransomware or malware attack, the Division/Program must report the incident to the Chief Information Office Bureau, Departmental Information Security Officer/Team via email Informationsecurity@ dmh.lacounty.gov as soon as the incident is discovered.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)

Passed in 2009 to encourage the use of electronic health records (*EHRs*). The HITECH Act strengthens HIPAA privacy and security protections. HITECH gives Health and Human Services (*HHS*), the authority to establish programs to improve healthcare quality and safety. The HHS also enforces HIPAA standards and regulations.

HITECH Breach Notification Rule

If a reportable Breach occurs and impacts more than 500 individuals, the Privacy Office must work with other County agencies to:

- Provide breach notification to impacted clients within 60 days upon discovery client PHI was accessed.
- Notify the Los Angeles County Chief Executive Office – Office of Privacy (*CEO-OOP*), Secretary of U.S. Department of Health and Human Services – Office for Civil Rights (*via*

CEO-OOP), and the California Office of the Attorney's General; and provide a substitute notice to the Department's external website and notify prominent media outlets.

The Privacy Office (PO)must keep all risk assessments, breach reports, and notifications for seven (*7*) years. The PO is also responsible for an accounting of disclosures for all Privacy and Security breaches that have impacted clients' PHI.

COMPLAINTS, DISCIPLINARY ACTIONS ANS SANCTIONS

DMH is a covered entity and required by law to investigate noncompliance with privacy and security policies and regulations and to impose disciplinary actions/sanctions equitably, progressively, and commensurate with the severity, frequency, and intent of violations without regard to classification, role or position.

The penalties for noncompliance with HIPAA are set in the Federal and State regulations. Penalties are based on the level of negligence and can range from $100 to $100,000 per violation (*or per record*), with a maximum penalty of $1.5 million per year for violations of an identical provision. Violations may also result in jail time for up to 10 years. Fines for violations of CMIA can be even higher and aggrieved clients may file lawsuits.

Disciplinary actions will not be applied to a workforce member who discloses PHI/PII to a health oversight agency or attorney in the process of reporting an allegation of unlawful conduct by the entity or violation of professional standards or clinical standards, or conditions in the entity that endanger clients (*whistleblower*), provided the disclosures are made in good faith.

While as a covered entity DMH is required to impose disciplinary actions for non-compliance, assessment of appropriate disciplinary action not clearly defined by State and Federal laws will consider system as well as individual factors that may have contributed to the violation.

Disciplinary actions for noncompliance can include, but are not limited to:

- Verbal/Written warnings.
- Loss of access
- Suspension without pay.
- Demotion
- Termination of employment.

For more information, please refer to DMH Policy 506.02 Privacy Sanctions.

Refraining from Intimidating or Retaliatory Acts

Workforce are prohibited from retaliating against any employee that reports a privacy incident, violator and/or breach. DMH has a non-retaliation policy and must promptly investigate reports or complaints that DMH or a workforce member acted to intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who exercises their rights under HIPAA or participates in any process established by HIPAA, including, but not limited to: filing complaints, testifying, assisting or participating in an investigation, a compliance review, a proceeding, or a hearing, or opposing any act or practice that is unlawful under HIPAA.

For more information, refer to DMH Policy No. 501.05, Refraining from Retaliatory or Intimidating Acts Against Individuals That Assert Rights Under HIPAA.

Waiver of Individual Rights

DMH does not require a client to waive their right to file a complaint or other rights regarding their PHI as a condition for the provision of treatment, payment or employment.

Clients who believe they have been treated in a manner that violates their rights may file a complaint with the Division/Program, Privacy Officer, Patients' Rights Advocates or with the Secretary of the Health and Human Services – Office for Civil Rights.

For more information, refer to DMH Policy No. 501.09, Prohibiting Offer of Treatment on the Condition of Waiver of Rights Under HIPAA.

WORKFORCE TELEWORK PROTOCOL

Remote Access/Working Offsite

When telecommuting, workforce is required to use a County issued VPN to securely access the County network remotely. Work must be conducted in an area with adequate privacy and security safeguards in place to ensure PHI/PII is not accessible to unauthorized persons/family. Workforce must never use public WIFI internet access. PHI/PII must be secured in a locked storage container or room when not in use, or on a County issued encrypted device. PHI/PII must not be saved on personal or home computers.

If an employee has not been issued a county laptop, home computers are permittable only when it has been equipped with up-to-date antivirus software, security applications and operating systems, and firewall software. Only county-related business must be conducted through the DMH desktop. These systems must be physically inaccessible to others and secured with DMH issued login credentials and multi-factor authentication verification.

WORKFORCE HIPAA TRAINING

HIPAA Compliant Training

Workforce members must take HIPAA training within the first 30 days of hire, or prior to accessing PHI, whichever comes first, and repeat every two years thereafter. They must complete three (3) mandatory trainings; HIPAA Covered Entities, Privacy Awareness and Cybersecurity Awareness training. The trainings support employees' education of legal, ethical and knowledge-based information required for protecting the clients' privacy as well as their sensitive and confidential information.

For more information, refer to DMH Policy No. 553.01, Privacy and Security Awareness Training.

INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM (*IBHIS*)

IBHIS is the electronic clinical record for DMH. IBHIS integrates a broad range of functionality including referral management, client registration, appointment scheduling, clinical documentation, workflow support, authorization, billing, claiming and reporting, along with providing the base for the electronic exchange of clinical information with other healthcare providers. Workforce access to IBHIS must be pre-approve by management and the Department's Clinical Informatics Division. Privacy Office often accesses IBHIS to verify an individual is a DMH client and determine status in relation to receiving mental health services.

Mitigation

DMH must mitigate, to the extent practicable, any known harmful effects that arise out of the wrongful use or disclosure of PHI or other HIPAA violations, either by members of its workforce or its business associates.

Workforce member should report suspected HIPAA violations to their supervisor or PO for investigation. Any violations must be mitigated by the Division/Program, including but not limited to, procedural changes, retraining, and/or disciplinary action/sanctions.

For more information, refer to DMH Policy No. 506.01, Mitigation of Harm.

Serious Threat

DMH may share patient information with anyone as necessary to prevent or lessen a serious threat to the health and safety of a person or the public – consistent with applicable laws and the standards of ethical conduct.

Therefore, if a workforce member reasonably suspects that a patient has committed a crime at a DMH facility, they may report it to law enforcement but should limit information to the circumstances of the incident, patient's name, address, date of encounter, and the individuals last known whereabouts.
For more information, refer to DMH Policy no. 500.02, Use and Disclosures of Protected Health Information Not Requiring an Authorization.

BUSINESS ASSOCIATE AGREEMENTS AND LIMITED DATA SET/USE AGREEMENTS

Business Associate Agreement (*BAA*)

A Business Associate is a person or organization that, on behalf of DMH, performs any function or activity covered by HIPAA related to payment and/or healthcare operations or provides a service involving the creation, maintenance, receipt, or transfer of PHI.

Examples of activities/services include accreditation, billing, data aggregation/analysis, document storage/destruction, patient safety activities, utilization review, IT systems, and repair/service of medical equipment.

Business Associate Agreements (*BAA*) with its designated Business Associates, are executed in accordance with HIPAA requirements.

DMH shall not disclose PHI to any contractors or vendors in the absence of a BAA. BAAs are not required for DMH's covered workforce, healthcare providers for treatment purposes, or clients/entities who may obtain incidental disclosures of PHI where access to PHI is minimal and not part of the clients'/entities job (*e.g., custodial and maintenance workers*).

For more information, refer to DMH Policy No. 507.01, HIPAA Business Associates.

Limited Data Sets/Data Use Agreement

DMH must enter into a Data Use Agreement with a researcher when disclosing limited data sets for research or health care operations, to establish permitted uses and disclosures, limit who can use or receive the data, and require the recipient to safeguard the information and not identify or contact the individual.

A limited data set excludes specified identifiers of the individual or of relatives, employers, or household members of the individual. Limited data sets are not subject to HIPAA's Accounting of Disclosures provisions. However, unauthorized uses or disclosures of a limited data set may constitute a HIPAA breach and must be investigated and reported.

For more information, refer to DMH Policy No. 500.04, De-Identification of Protected Health Information and Use of Limited Data Sets.

PERMITTABLE/NON-PERMITTABLE USES OF PHI

Fundraising and Marketing

In general, DMH is prohibited from using clients' PHI for fundraising purposes. DMH Workforce must obtain a signed authorization for any use or disclosure of PHI for marketing purposes, unless limited in accordance with DMH Policies. (*refer to Policy No. 500.01, Use and Disclosure of Protected Health Information Requiring Authorization, for additional information*)

Research

DMH permits the use and disclosure of PHI for research purposes only as follows:

- If the client who is the subject of the PHI provides prior written authorization
- Without the client's prior authorization when:
    - An Institutional Review Board has approved a waiver of the consent/authorization requirement.
    - Representations are obtained from the researcher that the use or disclosure of PHI is solely for preparation of the research.
    - PHI is de-identified in compliance with HIPAA's de-identification requirements or a limited data set is used.
    - Representations are obtained from the researcher that the use or disclosure of PHI is solely for the research on the PHI of decedents.

For more information, refer to DMH Policy No. 500.05, Use and Disclosure of Protected Health Information for Research and DMH Policy No. 500.04 De-Identification of Protected Health Information and Use of Limited Data Sets.

De-Identification of PHI

When health information does not identify a client, and there is no reasonable basis to believe that it can be used to identify a client, it is considered "de-identified," and it is not considered to be PHI. There are two (2) methods by which PHI may be considered de-identified: 1) Deletion of 18 specified identifiers and 2) DMH has no actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

For more information, refer to DMH Policy No. 500.04, De-Identification of Protected Health Information and Use of Limited Data Sets.

SENSITIVE PROTECTED HEALTH INFORMATION

Substance Use Disorders

Information pertaining to substance abuse clients is subject to special protection under both Federal and State laws.
42 CFR Part 2 prohibits the disclosure of substance abuse records to be used, to initiate, or to substantiate any criminal charges against a patient, or to conduct any investigation of a patient. However, a court order may authorize disclosure of confidential communications made by a patient to a program during diagnosis, treatment, or referral for treatment, only if:

- The disclosure is necessary to protect against an existing threat to life or of serious bodily injury (*e.g., suspected child abuse/neglect, verbal threats against third parties*).
- The disclosure is necessary for an investigation or prosecution of a serious crime (*e.g., homicide, rape, child abuse/neglect*); or
- The disclosure is for litigation or an administrative proceeding in which the patient offers testimony or other evidence pertaining to the content of the confidential communications.
- The disclosure is for a court ordered subpoena of client medical records.

Mental Health Records

Mental Health Records can be used or disclosed without a signed authorization for the purpose of treatment, payment, healthcare operations, and as required by State law. However, both HIPAA and State law require requests for medical records or PHI/PII that do not meet these requirements, must be accompanied with a signed authorization from the client, a subpoena or a court order. Requests for medical records shall be forwarded to the Health Information Management Division.

Health Information Management (HIM) Contact:

HIM Assistant Director
Olga Birov
Obirov@dmh.lacounty.gov
DMHHIM@dmh.lacounty.gov
(213) 943-8271

Privacy Office Contact

Privacy Officer
Maurnie V. Thomas
MEdwards@dmh.lacounty.gov
Privacy@dmh.lacounty.gov
(213) 943-937

ATTACHMENT A

LOS ANGELES COUNTY
DEPARTMENT OF MENTAL HEALTH
HIPAA PRIVACY INCIDENT/BREACH REPORTING FORM

Disclaimer:

The information provided in this form is intended to report potential privacy incidents or breaches. The report includes important information that shall be used solely for the purpose of reporting the possible violations of clients rights to privacy and protected health information.

The purpose of this form is to ensure that incidents are properly documented, investigated and addressed according to applicable federal and state privacy laws and Department of Mental Health (DMH) privacy policies and procedures. Please be assured that all information provided in this report will be treated with the highest level of confidentiality and only shared with authorized personnel involved in the investigation and resolution of the reported incident. By submitting this form, you acknowledge that you have read the aforementioned disclaimer and understand that you may be contacted for additional information as needed.

Date of Report: _____, 20___

1. PERSON FILING THIS REPORT

Full Name: _____Title: _____

Phone: (____) _____-_____E-Mail: _____

2. THE INCIDENT

Date of incident: _____, 20____Time: ____:____ ☐ AM ☐ PM

Describe the device(s) affected: _____

Name of staff allegedly responsible or involved in the incident. _____

Has staff completed the HIPAA Privacy/Security trainings? ☐ Yes ☐ No

Describe the incident (in full). Include location, date, time and name/email of staff involved:

3. PERSONAL HEALTH INFORMATION (PHI)

Was there client protected health information compromised by the incident? ☐ Yes ☐ No

If yes, how many clients impacted? _____

If available, please attach a list of the clients' names and addresses.

Type of protected information used/disclosed without authorization. (Check all that apply)

- ☐ Name
- ☐ Address
- ☐ Date of Birth
- ☐ Medical record number
- ☐ Social Security Number
- ☐ Diagnosis/Condition
- ☐ Medication
- ☐ Other _____

4. CONTAINMENT

What mitigation steps have been taken (staff counseling, deleted e-mails, etc.)?

5. IMPACTED SERVICES

Has the incident resulted in an interruption of client services? ☐ Yes ☐ No

If yes, please describe:

6. OTHER

Is there any other information you would like to include? ☐ Yes ☐ No

If yes, describe:

7. PERSON FILING REPORT

Signature: _____ Date:

Print Name: _____

-