DMH AI (Artificial Intelligence) Policy

Prepared by DMH Information Security

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

Los Angeles County Department of Mental Health Information Security Policy

Version: 3.1
Effective Date: TBD

Document Control

This is a controlled document produced by DMH CIOB. The control and release of this document is the responsibility of the DMH CIOB document owner.

Owner Details	
Name	Anthony Cabrera – DISO II
Department	DMH CIOB
E-mail Address	AtCabrera@dmh.lacounty.gov

Revision History			
Issue	**Date**	**Author**	**Comments**
V1	06/01/2025	Anthony Cabrera	Initial creation
V2	06/15/2025	Anthony Cabrera	Flow modification
V3	07/10/2025	Anthony Cabrera	Included Gartner review
V3	08/15/2025	James Thurmond	Review
V4	08/25/2025	Victor Ponce	Reorder policy flow and add appendix
V5	10/10/2025	Victor Ponce	Approved by management and Gartner

---

1. Purpose

This policy establishes the Artificial Intelligence (AI) information security framework for DMH to ensure the confidentiality, integrity, and availability of information assets, including electronic Protected Health Information (ePHI). It prioritizes emerging threats, particularly those introduced by (AI), by establishing rigorous security standards and vendor oversight to ensure compliance with the HIPAA Security Rule and NIST SP 800-53 Rev. 5 and other relevant frameworks.

---

2. Scope

This policy applies to all employees, contractors, systems, and third-party vendors or partners who access or manage DMH information systems or data, including systems that incorporate or interface with AI or machine learning technologies. It governs all information assets, whether on-premises, in the cloud, or integrated through external services.

---

3. Policy Requirements

3.1 Artificial Intelligence (AI) Risk Management

All partners must fill out the ***DMH AI (Artificial Intelligence) Assessment,*** for review and approval of the use AI, and to identify any potential security gaps.

All AI systems, whether developed in-house or procured from third parties, must be reviewed for risk including:

- Output inaccuracy, hallucination, or unjustified confidence
- Model bias affecting clinical or administrative decisions
- Unauthorized disclosure or misuse of ePHI via prompts or data sets
- Adversarial input attacks or prompt injection
- Data poisoning or model inversion during training or inference
- Ethical and regulatory implications of automated decision-making

All AI tools must:

- Comply with HIPAA and NIST 800-53 control requirements
- Be documented in the system asset inventory to include
    - Name
    - Vendor
    - Version
- Include logs of inputs, decisions, and outputs (AU-12)
- Have explainable AI features and mechanisms to detect performance drift (SI-4(14)). For example the predictions becoming less accurate as new data deviates from the data it was trained on, leading to flawed decision making, and inaccurate predictions.
- Be subject to the same change management, monitoring, and incident response as other critical systems (refer to internal policies, procedures and standards).

3.2 Third-Party AI Vendor Requirements
Any vendor, contractor, or business partner seeking to provide or integrate AI tools as part of a service to DMH must meet the following:

- Submit a **detailed use case** including how AI is used, what data it will process, and the purpose of automation
- Explain which AI security controls are in place. The following are examples:
    - Role-based access controls (AC-3)
    - Encryption mechanisms (SC-12, SC-28)
    - Logging/auditing systems (AU-12)
    - Model validation, fairness testing, and ethical review

- Deliver **evidence of independent third-party security assessments** from a recognized assessor, attesting to:
    - Alignment with **NIST AI Risk Management Framework (AI RMF)**
    - Mitigation of known issues from **OWASP Top 10 for LLMs**
    - Compliance with **HIPAA Security Rule**
    - Integrity and explainability of the AI's outputs

The documentation must be reviewed by the Information Security Office (DISO) and Privacy Office before the vendor is approved for:

- Access to DMH systems or data
- Contract execution or renewal
- Data exchange involving ePHI or sensitive business information

Failure to provide this validation may result in:

- Suspension of integration or onboarding
- Contract termination
- Security incident classification and escalation

3.3 Internal Use of AI Tools
Employees and contractors may not:

- Use public or unvetted AI platforms (e.g., ChatGPT, Bard, Copilot) to process, analyze, or store PHI/PII.
- Input sensitive or regulated data into AI systems without prior written authorization from the CISO and Privacy Officer

Approved AI tools must:

- Be registered and authorized by the IT department
- Be used in accordance with training and acceptable use guidelines

---

4. Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO)	Oversees AI and cybersecurity integration, vendor risk review, and control enforcement

Role	Responsibilities
Privacy Officer	Ensures AI tools comply with HIPAA Privacy and Security Rules; reviews BAAs
AI System Owners / Developers	Document, validate, and monitor AI tools for compliance and ethical use
IT Department	Manages infrastructure, access controls, and system monitoring
All Workforce Members	Use only approved AI systems, follow data handling and security protocols

---

5. Enforcement

Violations of this policy—especially involving AI misuse, unauthorized data input, or failure to validate AI vendors—will be subject to disciplinary action up to and including:

- Employment termination
- Contract suspension or cancellation
- Mandatory HIPAA breach reporting
- Legal or regulatory sanctions

Third-party vendors who fail to submit third-party security validation or demonstrate insufficient AI safeguards will be disqualified from handling sensitive data and may face contract non-renewal or immediate termination.

---

6. Review and Updates

This policy shall be reviewed by the Information Security and Compliance teams, and updated as necessary to reflect changes in:

- Legal or regulatory requirements (e.g., HIPAA, NIST updates)
- Organizational AI strategy
- Industry best practices (e.g., NIST AI RMF revisions)

Appendix A

HIPAA Security Rule – Relevant Requirements

HIPAA Rule Section	Requirement Description
164.308(a)(1)(ii)(A)	Conduct accurate and thorough risk analysis, including AI systems
164.308(a)(5)(i)	Implement security awareness training, including AI-related risks
164.308(a)(8)	Perform regular evaluations of AI-enabled systems and controls
164.310(c)	Limit physical access to information systems used for AI model training or deployment
164.312(a)(1)	Implement access controls for AI interfaces and model endpoints
164.312(b)	Implement audit controls that log and review AI model inputs and outputs
164.312(c)(1)	Protect data integrity, including against adversarial AI manipulation
164.312(e)(1)	Secure transmission of ePHI to or from AI tools or APIs
164.314(a)(1)	Ensure Business Associate Agreements (BAAs) address AI tool risks and safeguards

NIST SP 800-53 Rev. 5 – Applicable Controls

NIST Control ID	Control Name	Description
RA-3	Risk Assessment	Include AI-specific risks in enterprise-wide security assessments
PL-8	Security and Privacy Architectures	Ensure AI systems are reviewed as part of overall IT architecture
AC-3	Access Enforcement	Limit access to AI models, prompts, and data sets based on roles
AU-12	Audit Generation	Require logging of AI interactions and decisions
SI-4	System Monitoring – Unauthorized Use	Detect misuse or anomalous behavior in AI systems
SA-8(11)	Security Engineering Principles – AI Considerations	Require development, validation, and testing controls for AI
SC-28	Protection of Information at Rest	Ensure AI training data and model artifacts are encrypted

NIST Control ID	Control Name	Description
SC-12	Cryptographic Key Establishment	Required for secure encryption of AI data and communications
IA-2	Identification and Authentication	Use MFA for access to AI tools handling ePHI or critical data
SA-12	Supply Chain Protection	Enforce AI security validation in third-party vendors and partners