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

DMH AI (Artificial Intelligence) Assessment

Prepared by DMH Information Security

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

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

Statement on the Responsible Use of Artificial Intelligence and Information Security Program Partner Requirements

Artificial Intelligence (AI) Users

As part of our ongoing commitment to ethical innovation and information security, the Department of Mental Health (DMH) affirms our principles for the responsible use of Artificial Intelligence (AI) in all areas of our operations. Our approach is grounded in transparency, accountability, and strong cybersecurity practices to safeguard both our data and yours. Our shared responsibility depends on the cybersecurity strength of our partners, and as such, we consider these guidelines minimum requirements for our partners

Key Principles and Commitments

1. Responsible and Ethical Use of AI

- We (DMH) utilize AI technologies strictly in accordance with legal, ethical, and regulatory standards.
- AI systems are implemented with human oversight, transparency, and explainability, especially where output influences business decisions.
- We actively monitor AI models for potential *bias*, *misuse*, or *unintended* consequences.
- The use of DMH data for training or fine-tuning AI learning models—whether internal or external, is *strictly prohibited*. DMH data shall only be used for defined operational purposes and may not be included in any AI datasets or model development activities.

2. Data Protection and Sovereignty

- DMH adheres strictly to data residency requirements and ensure that no business, customer, or partner data is stored or processed outside the United States, unless contractually agreed upon and legally compliant.
- All third-party AI tools and platforms undergo rigorous security and compliance assessments, including data flow transparency and geographic storage validation.
- Continuously test for unintended release of information due to prompt injection.

3. Robust Information Security Program

- Our security framework is based on leading industry standards and regulatory requirements, including the NIST Cybersecurity Framework, and the HIPAA Security and Privacy Rules, where applicable.
    - We maintain a layered defense-in-depth strategy including, but not limited to:
        - Regular risk assessments and third-party audits
        - Network segmentation
        - Data encryption (in transit and at rest)
        - Continuous monitoring and anomaly detection
        - Strict access controls and identity management
        - Mandatory employee cybersecurity awareness training to promote a security-first culture and reduce human risk vectors.
- AI systems are subject to specific threat modeling and secure development lifecycle (SDLC) controls.

4. Third-Party and Supply Chain Security

- All vendors, including those providing AI capabilities, must meet our security and compliance requirements through contractual obligations and ongoing due diligence.
- *We prohibit unauthorized data sharing* with third parties and implement controls to prevent data leakage or misuse.

5. Incident Response and Governance

- A dedicated AI governance and security team ensures adherence to AI-specific risk policies.
- Our incident response plan is regularly tested and includes AI-related threat scenarios (e.g., model poisoning, data exfiltration through AI inputs/outputs).
- Business continuity and disaster recovery plans include contingencies for AI system failures or compromises.

We recognize that AI presents both opportunities and new risk vectors. Our commitment is to proactively address these risks while maintaining the highest standards of integrity, privacy, and cybersecurity. We invite open dialogue with our partners to continuously improve and align our shared values in a rapidly evolving digital environment.

For any questions or to request more details about our AI and INFOSEC governance, please contact our Information Security team.

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

Self-Assessment Checklist

Responsible Use of Artificial Intelligence and Information Security Program Partner Requirements

Purpose Statement: Secure Implementation of Artificial Intelligence (AI)

Artificial Intelligence (AI) is increasingly becoming a critical component of modern business operations, the Los Angeles County Department of Mental Health (DMH) is committed to ensuring its responsible and secure implementation. The purpose of this document is to establish a clear expectation for all business partners (contract providers) to adopt AI practices that uphold the confidentiality, integrity, and availability of shared information.

We recognize that the security of AI systems is a **shared responsibility**, and any weaknesses across our partnerships can present a universal risk. Therefore, we provide the following **self-assessment checklist** as a **minimum standard** for evaluating the security posture and risk profile of any AI implementation.

All partners are expected to use this checklist to assess compliance with **AI and Information Security Principles** and identify areas for improvement. This risk assessment will be reviewed by DMH Security teams.

AI Security Self-Assessment Checklist

Current Use of AI in your organization

Is AI currently in use in your organization? If so, please ***state business case***, vendor of choice and any relevant details regarding the security of this AI model in the box below:

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

For the Questionnaire, any questions answered as “No” or “N/A” will require an explanation.

A. Governance & Ethical Use	**Yes**	**No**	**N/A**
Are you currently addressing the challenges of output inaccuracy, hallucination, or unjustified confidence in your models?			
Is the use of partner data to train or fine-tune AI models ***explicitly prohibited****?*			
Is human oversight in place for all AI-driven decision-making processes?			
Does a review process exist to *evaluate bias*, *misuse*, or *unintended consequences* of AI outputs?			
Are these systems subject to the same change management, monitoring, and incident response protocols as your other critical systems?			
B. Data Protection & Sovereignty	**Yes**	**No**	**N/A**
Can you ensure that ***No DMH data*** is stored or processed outside of the United States without express written approval?			
Do all AI platforms and tools undergo security and compliance assessments, including data flow validation?			
Are controls in place to detect and prevent prompt injection vulnerabilities?			
Is encryption applied to all sensitive data (in transit and at rest)?			
Are outputs checked for inaccuracy, hallucination, or unjustified confidence?			
C. Security Program Alignment	**Yes**	**No**	**N/A**
Does your information security program follow NIST, or HIPAA frameworks, where applicable?			
Are your incident Response plans practiced?			
Is access to AI systems and data tightly controlled and monitored?			

Is security awareness training, including topics on AI risks—mandatory for all employees?			
Are secure development lifecycle (SDLC) practices followed for all AI model development?			
Are you ensuring compliance with HIPAA and NIST 800-53 control requirements for these systems?			
Can you confirm that these systems include logs of inputs, decisions, and outputs as required by AU-12?			
Are there mechanisms in place to provide explainable AI features and detect performance drift, aligning with SI-4(14)?			
D. Vendor and Supply Chain Risk	**Yes**	**No**	**N/A**
Are third-party AI vendors contractually obligated to meet security and privacy requirements?			
Are controls in place to detect and prevent unauthorized data sharing or leakage?			
E. Incident Response and Continuity	**Yes**	**No**	**N/A**
Are AI-related risks incorporated into the organization's incident response plan?			
Does the incident response plan include scenarios for model corruption, data poisoning, and system failure?			
Does business continuity and disaster recovery procedures account for AI dependencies?			

Submission and Remediation

Partners should retain a copy of the completed checklist and submit it to DMH Information Security Office. Identified gaps must be addressed through a documented remediation plan with timelines.