# Document Metadata

author: jfraze@mycomp.org

title: Third-Party Generative AI Vendor Risks

nist\_function: Manage

priority\_phase: Must

last\_reviewed: 2025-06-24

status: draft

## **Purpose**

To govern and mitigate risks associated with the use of third-party generative AI tools, APIs, or models integrated into hospital systems, ensuring security, compliance, and trustworthiness.

## **Scope**

Covers all third-party GenAI tools, APIs, SaaS platforms, and hosted LLM services procured or integrated into hospital IT environments—including virtual scribes, chatbot assistants, clinical summarizers, and analytics models.

## **Policy Statement**

Third-party GenAI systems must undergo security, provenance, and risk posture evaluation aligned with NIST SP 800-218A, NIST AI RMF, and AI 600-1 controls before deployment or contract execution. Vendor services must demonstrate compliance with data handling, inference boundary controls, and misuse prevention standards.

## **Roles and Responsibilities**

• Procurement and Legal: Require vendor attestation to AI usage, training data sources, and security practices.

• Information Security: Perform risk assessments of APIs, SDKs, and hosted model interfaces.

• Clinical Informatics: Validate that vendor outputs are appropriate for intended healthcare contexts.

• Vendor Management: Track contractually required SLAs for drift monitoring, update notification, and incident reporting.

## **Implementation Phases**

### **Must Do**

• Require SBOM-equivalent for model artifacts: base model lineage, fine-tuning steps, and plugin metadata (SP 800-218A §3.3).

• Enforce data boundary controls: confirm vendor cannot store PHI unless explicitly permitted.

• Conduct vendor-hosted model red-team simulation or require result disclosure.

• Review third-party GenAI provider’s incident response and model update policies (NIST 800-61r3 alignment).

### **Should Do**

• Mandate logging and access control auditability for any model capable of PHI inference.

• Verify existence of misuse detection systems (e.g., prompt abuse, re-identification, LLM jailbreaks).

• Check for vendor transparency disclosures (e.g., OpenAI System Card, Google Vertex AI summaries).

### **Recommended**

• Maintain internal registry of all GenAI vendors with risk tiering and deployment zones.

• Participate in third-party risk exchanges or threat-sharing networks for LLM misuse signals.

• Require model performance degradation SLAs or alert thresholds.

## **References**

• NIST SP 800-218A §3.3, §5.2

• NIST AI RMF: GOVERN-4, MANAGE-2.3, MANAGE-4.2

• NIST AI 600-1: §2.2.2, §2.5

• Top Vulnerabilities: #12 Supply Chain, #18 Misuse, #16 Alignment Drift

## **Review Cycle**

• Prior to initial contract signing

• At model version change, interface upgrade, or change in hosting vendor