# Document Metadata

author: jfraze@mycomp.org

title: Policy Enforcement Phases for AI Risk Controls

nist\_function: Govern

priority\_phase: Must

last\_reviewed: 2025-06-24

status: draft

## **Purpose**

To define phased enforcement of AI and generative AI (GenAI) risk controls across the organization, mapping minimum, recommended, and maturity-aligned requirements for compliance and risk reduction.

## **Scope**

Applies to all AI/GenAI systems evaluated, deployed, or integrated within hospital environments—including patient-facing systems, clinical support tools, administrative automation, and embedded APIs.

## **Policy Statement**

All AI risk management practices shall be applied using a tiered enforcement approach:  
- Must Do: Minimum safeguards required for deployment.  
- Should Do: Recommended practices to enhance trustworthiness.  
- Recommended: Advanced maturity measures for continuous assurance and high-risk environments.

## **Roles and Responsibilities**

• AI Governance Committee: Establishes phase definitions and enforcement scope.

• IT & Security Leadership: Integrates phase thresholds into system onboarding.

• Clinical Stakeholders: Validate that controls are appropriate to clinical context.

• Compliance Officers: Monitor adherence to baseline and advanced requirements.

## **Implementation Phases**

### **Must Do**

• Implement AI RMF core functions across all GenAI systems (GOV-1 through MANAGE-4).

• Enforce role separation, model validation, hallucination mitigation, and PHI boundary controls.

• Require documented use case scope, auditability, and pre-deployment testing (AI 600-1 §2.1–2.4).

### **Should Do**

• Apply fairness metrics, human-in-the-loop review, and risk telemetry logging.

• Align with ONC and HIPAA technical safeguards and CSF 2.0 cybersecurity controls.

• Conduct annual risk profile reassessment and update enforcement phases.

### **Recommended**

• Implement model-specific governance artifacts, fallback routines, and drift analytics.

• Use GenAI-specific explainability layers and chain-of-responsibility logging (AI 600-1 §2.5).

## **References**

• NIST AI RMF 1.0: GOVERN-1, MANAGE-1.1, MAP-1.5

• NIST AI 600-1: §2.1, §2.3.1, §2.4.1

• HIPAA Security Rule §164.308

• CSF 2.0 Governance & Oversight Functions

## **Review Cycle**

Reviewed annually or when system scope or regulatory guidance changes.