# Document Metadata

author: jfraze@mycomp.org

title: AI Risk Management Policy Overview

nist\_function: Govern

priority\_phase: Must

last\_reviewed: 2025-06-24

status: draft

## **Purpose**

To establish a foundational policy framework for managing risks associated with artificial intelligence (AI) and generative AI (GenAI) technologies used across hospital operations, ensuring alignment with trustworthiness principles, sectoral regulations, and NIST AI RMF guidelines.

## **Scope**

Applies to all AI/GenAI systems, including clinical documentation tools, decision support systems, patient interaction bots, and administrative applications in the healthcare environment.

## **Policy Statement**

Hospitals must implement AI risk management practices aligned to NIST AI RMF 1.0 and AI 600-1. This includes identification, assessment, mitigation, and monitoring of AI risks throughout the lifecycle. Trustworthiness goals (e.g., fairness, transparency, robustness) shall guide all GenAI uses.

## **Roles and Responsibilities**

• Hospital Board: Ultimate accountability for AI oversight.

• CIO / CISO: Operationalize policy via IT and security teams.

• AI Ethics Committee: Oversee model risks, bias, and safety.

• Clinical Leadership: Ensure AI aligns with patient care quality and safety.

## **Implementation Phases**

### **Must Do**

• Define GenAI as a distinct class of risk-bearing software (§AI 600-1 Introduction).

• Require risk management for all AI systems touching PHI or patient decision pathways.

• Adopt NIST AI RMF Core Functions (GOV, MAP, MEASURE, MANAGE).

### **Should Do**

• Integrate GenAI policy into cybersecurity and software development governance (CSF 2.0, SP 800-218A).

• Align AI/GenAI policies with ONC certification and HIPAA compliance.

### **Recommended**

• Link AI RMF risk criteria to hospital quality assurance, MIPS/MACRA, and safety committees.

## **References**

• NIST AI RMF: GOVERN-1.1, GOVERN-1.2

• NIST AI 600-1: §2.1, §2.4.2

• HIPAA §164.308; CSF 2.0 "Govern"

## **Review Cycle**

Annually, or when AI deployment types or applicable regulations change.