# Document Metadata

author: jfraze@mycomp.org

title: AI Policy Management Templates

category: Appendices

last\_reviewed: 2025-06-24

status: draft

# **AI Risk Management Policy Templates**

This appendix provides editable templates that hospital stakeholders may use to standardize intake, assessment, governance, and response activities related to AI and generative AI systems. These are designed to align with the NIST AI RMF (GOV, MAP, MEASURE, MANAGE) and AI 600-1 (§2.1–2.5) controls.

## **1. AI/GenAI Use Case Intake Form**

Purpose: Collect necessary details to assess risk, context, and governance requirements for any new or proposed AI/GenAI system.

Template Fields:  
- Use Case Name:  
- Requesting Department:  
- Primary Contact:  
- Intended Purpose:  
- System Type: (e.g., LLM, diffusion model, NLP assistant)  
- Deployment Mode: (internal / vendor-hosted / embedded)  
- Patient Impact Level: (Low / Medium / High)  
- Involves PHI? (Yes / No)  
- Regulatory Category (if applicable): SaMD / eCQMs / administrative  
- Known Risks (hallucination, prompt injection, etc.):  
- Expected Benefits:  
- Human Oversight Plan:  
- Data Sources Used:  
- Review Date:  
- Review Body: (e.g., AI Governance Committee)

## **2. AI Bias Impact Assessment Template**

Purpose: Document the risk of bias or fairness issues associated with model behavior, outcomes, or data inputs.

Template Fields:  
- System Name and Version:  
- Description of Output:  
- Is output individualized (i.e., varies by demographic)?  
- Training Dataset Source(s):  
- Fairness Metrics Used:  
- Results Across Key Demographics:  
- Mitigation Techniques Applied:  
- Reviewer Comments:  
- Ethics Board Sign-Off: [Yes/No]  
- Last Updated:

## **3. AI Incident Report Form**

Purpose: Provide a structured record for reporting AI/GenAI-related safety events, errors, or ethical failures.

Trigger Examples: hallucination over threshold, prompt injection, model drift, PHI leakage

Template Fields:  
- Incident ID:  
- Affected System(s):  
- Incident Date:  
- Reporter Name:  
- Type of Incident: [ ] Hallucination [ ] Drift [ ] Prompt Injection [ ] PHI Leak [ ] Other  
- Description of Event:  
- Clinical Impact (if any):  
- Containment Action Taken:  
- Escalation Path:  
- Root Cause Analysis Summary:  
- Regulatory Reporting Required? (Yes / No)  
- Final Resolution:  
- Date Closed:

## **4. Prompt Library Risk Management Form**

Purpose: Track and manage prompts used in GenAI systems that influence patient-facing or safety-relevant outputs.

Template Fields:  
- Prompt ID:  
- Use Case:  
- Authorized User Group:  
- Prompt Text:  
- Risk Category: Low / Medium / High  
- Safety Filter(s) Applied:  
- Last Reviewed:  
- Revision History:  
- Reviewer Notes:

## **5. AI/GenAI Deployment Approval Checklist**

Purpose: Ensure a GenAI system has satisfied all governance, documentation, testing, and validation requirements prior to production deployment.

Checklist Items:  
- [ ] Context and use case documented (MAP-1.1)  
- [ ] PHI boundary controls verified (MANAGE-2.2)  
- [ ] Validation and hallucination testing completed (§2.3.1)  
- [ ] Explainability elements embedded (MEASURE-2.6)  
- [ ] Bias assessment performed (AI 600-1 §2.4.1)  
- [ ] Logging and drift monitoring configured (MANAGE-2.1)  
- [ ] Incident response pathway assigned (MANAGE-3.1)  
- [ ] Governance approval recorded  
- [ ] Deployment date:  
- [ ] Approval by:

## **Notes**

These templates should be version-controlled and incorporated into the hospital’s GRC, quality, or cybersecurity tracking systems. Customization is encouraged to reflect department-specific workflows.

## **References**

• NIST AI RMF Core (GOV‑1 through MANAGE‑4)

• NIST AI 600‑1 §2.1–2.5

• HIPAA §164.308 Security Rule

• FDA PCCP Guidance (2024)