AI Use Policy Template for Hospitals

Core Policy + Add-On Modules

Includes Rural Proofing Additions

August 2026

KANSAS HEALTH INSTITUTE

Informing Policy. Improving Health.

HEALTH WORKS

KANSAS HOSPITAL ASSOCIATION

KHI/26-71

About This Resource

The *AI Use Policy Template for Hospitals: Core Policy + Modules* (hereafter, the *AI Use Policy Template*) provides hospitals with a ready-to-complete AI use policy organized into clearly labeled sections with checkboxes and fillable fields. It guides organizations through defining how AI will be used, who the policy applies to and how to address allowable and prohibited uses using a risk-based framework. In this context, artificial intelligence (AI) refers to computer systems and technologies—ranging from predictive analytics to generative tools—that process data to perform tasks such as analyzing information, generating text or images, or supporting decisions and recommendations that would otherwise require human judgment. The *AI Use Policy Template* is intended as a starting point and should be adapted to reflect your organization's specific context, needs and applicable laws.

This *AI Use Policy Template* is accompanied by the *Companion to the AI Use Policy Template for Hospitals: Section-by-Section Guide* (hereafter, the *Companion Guide*). The *Companion Guide* provides detailed instruction for completing the policy and explains the purpose of each section, why it matters and considerations for selecting among the available options. Together, the *AI Use Template* and the *Companion Guide* are designed to support hospitals and health systems of varying sizes, capacities and levels of AI experience.

The *AI Use Policy Template* also supports rural proofing: throughout the document, specific checkboxes, fields and columns are included to capture rural-specific realities such as staffing constraints, limited broadband, smaller data volumes and greater distance to services. This allows hospitals to reflect their own rural conditions directly within the policy.

Authors

Tatiana Lin, M.A.
Director of Business Strategy and Innovation,
Kansas Health Institute

Emma Uridge, M.P.H.
Analyst,
Kansas Health Institute

Shelby C. Rowell, M.P.A.
Senior Analyst,
Kansas Health Institute

Acknowledgments

The *AI Use Policy Template* and the *Companion Guide* were developed by the Kansas Health Institute. Funding to support the development of these resources was provided by Healthworks.

The development of these resources built upon work previously completed by KHI through the Centers for Disease Control and Prevention (CDC) of the U.S. Department of Health and Human Services (HHS) Strengthening U.S. Public Health Infrastructure, Workforce, and Data Systems grant (OE22-2203). The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by CDC/HHS, or the U.S. Government.

The Kansas Health Institute supports effective policymaking through nonpartisan research, education and engagement. KHI believes evidence-based information, objective analysis and civil dialogue enable policy leaders to be champions for a healthier Kansas. Established in 1995 with a multiyear grant from the Kansas Health Foundation, KHI is a nonprofit, nonpartisan educational organization based in Topeka.

Healthworks serves as the nonprofit arm of the Kansas Hospital Association. Healthworks educates partners, brings groups together and finds funding to provide services to change health care for the better. Healthworks believes with bold ideas and brave leadership, anything is possible.

This template is available online at khi.org/articles/ai-use-policy-template-for-hospitals-and-companion-guide.

Legal Disclaimer

This *AI Use Policy Template* is intended for educational purposes only and does not constitute legal advice. It is not a substitute for consultation with legal counsel or other qualified professionals. Hospitals should consult their own legal and other advisors before adopting or implementing an artificial intelligence use policy and should adapt this *AI Use Policy Template* to meet the needs of their individual organization.

Because AI technologies, regulations and best practices continue to evolve, hospitals should regularly review and update their policies to ensure ongoing relevance and compliance. The authors make no representations or warranties of any kind, express or implied, regarding the content of this *AI Use Policy Template*. Links to third-party content are provided for reference only, and the authors do not guarantee the accuracy or reliability of information provided by third parties.

How to Use This Template

This *AI Use Policy Template* is divided into two parts:

Part 1 — Core Policy (*recommended for all hospitals*): Sections 1-19 cover governance, risk framework, training, prohibited use, vendor obligations and policy administration.

Part 2 — Add-On Modules (*recommended based on hospital needs*): Five standalone modules cover specific AI use cases. Each module is self-contained and slots into the policy immediately after Section 19.

This *AI Use Policy Template* uses a risk-based framework as the governing structure for all AI use. The add-on modules do not replace that framework. Instead, they provide additional requirements for selected AI use cases that may require more specific safeguards, documentation, oversight or operational guidance. Hospitals should include only the modules that apply to their current or planned AI tools.

Step 1: Open the Companion Guide

This *AI Use Policy Template* is accompanied by the *Companion to the AI Use Policy Template for Hospitals* (the *Companion Guide*). Open the *Companion Guide* alongside this *Template* and place the two documents next to each other. Refer to the *Companion Guide* as you work through each section to understand its purpose and the considerations behind each available option.

Step 2: Select Your Modules

Review each module below. Check the box if your hospital currently uses — or plans to use within 12 months — any of the described tools.

Add?	Module	Include this module if your hospital uses…	Common examples
☐	**Module A** Ambient Documentation AI	Any AI that generates or drafts clinical notes entered into the Electronic Health Record	Nuance DAX, Abridge, Suki, Epic ambient documentation
☐	**Module B** Diagnostic and Radiology AI	AI that reads, flags, or prioritizes imaging, pathology or lab results	GE Healthcare AI, Aidoc, Viz.ai, Epic radiology prioritization
☐	**Module C** Predictive Alerts and Clinical Decision Support	Sepsis models, deterioration alerts, readmission risk or AI-generated clinical flags in nursing/physician workflows	Epic Sepsis Model, Deterioration Index, EarlySense, BestPractice Alerts
☐	**Module D** Revenue Cycle AI	AI-assisted coding, prior authorization, claims editing or any function affecting Medicare/Medicaid billing	Optum360, Change Healthcare, Thrive, Epic coding AI
☐	**Module E** Generative AI and Productivity Tools	ChatGPT, Microsoft Copilot, Google Gemini, or similar tools for drafting, summarizing or administrative work	Microsoft Copilot for Microsoft 365, ChatGPT Enterprise, Claude for Enterprise, Gemini for Workspace. This category refers to enterprise or institutionally licensed AI tools procured, approved, and managed by the hospital or health system. Personal subscriptions or consumer versions of these tools are not covered by hospital data protection agreements and must not be used with hospital data unless explicitly approved.

Step 3: Assemble Your Policy

The *AI Use Policy Template* is organized as a series of bullet points with fillable checkboxes; check the boxes that apply to your hospital as you go. As you make decisions about which options to select, consider your hospital's needs, capacity, operational practices, and other relevant factors. Use your completed selections as the foundation for writing your policy.

Your final policy document consists of:

1. Part 1: Core Policy (Sections 1-19) — suggested for all hospitals
2. The Add-On Modules selected above — place after Section 19
3. Policy Approval Signatures, Staff Acknowledgment Form, Record of Revisions
4. Appendices A-F — Governance Contacts, AI Use Register, Disclosure Scripts, Regulatory References, Approved Tool Lists, Control Role Assignments

Step 4: Complete and Finalize

Work through Part 1 and each selected module, filling in all shaded blue fields and making checkbox selections.

Important:

- Have your Chief Compliance Officer (CO), Chief Medical Officer (CMO), Chief Nursing Officer (CNO) and Information Technology (IT) Security Officer review relevant sections.
- Engage your hospital's legal counsel on any contractual, HIPAA, or liability provisions.
- Smaller hospitals (CAH, <100 beds) may combine roles; larger systems may need separate owners per section.
- Delete all instructional text (in italics) before finalizing the policy.

Part 1

Core Policy

Suggested for all hospitals. Sections 1–19.

Hospital / System Name	
Policy Number (e.g., AI-2026-001)	
Version (start at 1.0)	
Approving Authority (Name / Title)	
Effective Date	
Next Review Date	

Section 1: Purpose

Describe why your hospital is adopting an AI policy and what outcomes it is intended to support.

This policy establishes requirements and standards for the responsible and ethical use of artificial intelligence (AI) within _____ (insert the full legal name of the "hospital or health system," then delete this parenthetical note). It provides a framework ensuring AI is implemented in ways that:

Check all that apply:

- ☐ Enhance patient safety and quality of care
- ☐ Support clinical decision-making without replacing clinicians judgment
- ☐ Protect patient privacy and comply with the Health Insurance Portability and Accountability Act (HIPAA)
- ☐ Build and maintain patient and community trust
- ☐ Support workforce efficiency and reduce administrative burden
- ☐ Advance health equity and reduce disparate care
- ☐ Other: _____

... while upholding the following principles:

- ☐ Human oversight and clinical accountability
- ☐ Transparency to patients, staff and regulators
- ☐ Data privacy and security
- ☐ Bias awareness and equity
- ☐ Regulatory compliance (HIPAA, Joint Commission, Centers for Medicare & Medicaid Services)
- ☐ Other: _____

Section 2: Scope

Check all AI technologies this policy governs. Include embedded electronic health record (EHR) system AI features even if not marketed as standalone AI tools.

This policy covers the following AI technologies used within the hospital:

- ☐ Clinical decision support (CDS) tools and AI-assisted diagnostics
- ☐ AI-assisted clinical documentation (ambient listening, natural language processing (NLP) scribe tools, auto-coding)
- ☐ Radiology/pathology AI (image analysis, flagging, triage)
- ☐ Predictive analytics (sepsis prediction, readmission risk, deterioration alerts)
- ☐ Generative AI (tools producing text, summaries, images, or code — e.g., ChatGPT, Copilot)
- ☐ Revenue cycle AI (coding assistance, prior authorization, claims review)
- ☐ Patient engagement/scheduling AI (chatbots, patient portals)
- ☐ Operational AI (staffing models, supply chain, capacity prediction)
- ☐ AI embedded in EHR or vendor platforms (e.g., Epic, Oracle Health [formerly Cerner] AI modules)
- ☐ Other: _____

Section 3: Applicability

3.1 Departments and Care Areas

This policy applies to (check all that apply):

- ☐ All clinical departments using AI tools in patient care or documentation
- ☐ Revenue cycle, coding and billing departments
- ☐ Radiology, laboratory and diagnostic services
- ☐ IT / health informatics departments procuring or managing AI systems
- ☐ Quality, compliance and patient safety offices
- ☐ Administration and operations
- ☐ Other: _____

3.2 Workforce Coverage

As you decide which workforce groups to include, consider who may use, access, support, oversee, procure, configure, manage, or otherwise interact with AI systems as part of their role.

This policy applies to all of the following individuals ("Covered Persons"):

- ☐ Physicians, Advanced Practice Providers (APPs) and all licensed clinical staff
- ☐ Nurses and nursing assistants
- ☐ Administrative and clerical staff
- ☐ IT and informatics staff
- ☐ Students, residents, fellows and trainees
- ☐ Contractors, consultants, and agency / travel staff
- ☐ Volunteers
- ☐ All of the above — referred to as "Covered Persons" throughout this policy

3.3 Vendors and Third Parties

Vendors, including EHR vendors, AI software providers, and cloud service providers are governed through procurement requirements, contract terms, Business Associate Agreements (BAAs), and vendor risk assessments. Third-party obligations are detailed in Section 14.

Section 4: Alignment with Existing Policies and Regulations

Check all applicable regulations and internal policies. Note internal policy numbers in Appendix D.

This policy shall be interpreted and enforced in alignment with the following. Where requirements conflict, the stricter standard applies.

- ☐ HIPAA Privacy and Security Rules (45 CFR Parts 160 and 164)
- ☐ The Joint Commission Standards (Leadership, Information Management, Patient Safety)
- ☐ CMS Conditions of Participation
- ☐ State-Specific Laws and Regulations (e.g., Kansas Hospital Licensure Regulations [K.A.R. 28-34])
- ☐ Hospital Information Security Policy
- ☐ Electronic Health Record (EHR) Governance Policy
- ☐ Medical Staff Bylaws (for clinical AI use)
- ☐ Records Retention and Destruction Policy
- ☐ Procurement / Vendor Management Policy
- ☐ Other: _____

Section 5: Guiding Principles

Select all principles the Hospital adopts. At minimum, select Patient Safety First, Human Oversight, Data Privacy, and HIPAA Compliance.

The Hospital is committed to the following principles guiding AI use:

- ☐ **Human Oversight and Clinical Accountability:** Clinicians retain full accountability for all AI-informed decisions. AI does not replace clinical judgment.
- ☐ **Patient Safety First:** AI shall not be deployed in clinical settings without validation, monitoring, and clear escalation protocols.
- ☐ **Transparency:** Patients will be informed when AI a significant influences their care. Staff will understand the tools they use.
- ☐ **Bias Awareness and Mitigation:** The Hospital will proactively identify, assess and address potential AI bias across race, ethnicity, age, gender, language, socioeconomic status, geography and rurality to help promote equitable outcomes and reduce the risk of unintended disparities. This includes assessing whether AI tools were developed, tested and validated using data that reflects rural populations, smaller patient volumes and the service conditions of this Hospital's community and documenting known limitations where such validation is unavailable.
- ☐ **Data Privacy and HIPAA Compliance:** Protected Health Information (PHI) will never be entered into AI tools without a valid BAA reviewed by the Privacy Officer.
- ☐ **Data Security:** AI systems and data will be protected per the Hospital's Information Security Policy and National Institute of Standards and Technology (NIST) standards.
- ☐ **Explainability:** The Hospital will prioritize AI systems that provide understandable, interpretable or reviewable outputs to support informed clinical, operational and oversight decisions.
- ☐ **Workforce Sustainability:** AI will enhance, not eliminate, clinical and operational roles.
- ☐ **Equity and Accessibility:** AI tools will be assessed for equitable performance and will comply with ADA requirements.
- ☐ Other: _____

Section 6: Key Definitions

These definitions apply throughout the policy. Add hospital-specific terms in the blank rows at the bottom.

Term	Definition
Artificial Intelligence (AI)	Computer-based systems that perform tasks typically requiring human intelligence, including clinical reasoning, pattern recognition, language understanding, and predictive modeling.
Clinical Decision Support (CDS)	AI or algorithmic tools providing clinicians with patient-specific evidence-based information, alerts, or recommendations at the point of care.
Generative AI (GenAI)	AI that creates new content — text, images, audio, code — in response to user prompts (e.g., Microsoft Copilot, ChatGPT).
Protected Health Information (PHI)	Individually identifiable health information held or transmitted by the Hospital in any form, as defined under HIPAA (45 C.F.R. § 160.103).
Business Associate Agreement (BAA)	A HIPAA-required written contract between the Hospital and any vendor that creates, receives, maintains, or transmits PHI on the Hospital's behalf.
Human-in-the-Loop (HITL)	A requirement ensuring a qualified human reviews and approves AI-generated outputs before they influence a patient care decision or official action.
AI Use Register	The Hospital's centralized inventory of approved AI tools documenting tier, security level, BAA status, and oversight owner. Maintained in Appendix B.
Procured AI Tool	An AI platform formally acquired by the Hospital through an approved procurement process with completed security, privacy, and BAA reviews.
Publicly Accessible AI Tool	Commercially available AI not procured by the Hospital (e.g., individual Claude , free-tier tools). PHI and confidential data must never be entered.
Risk Tier	A classification — Tier A (High Risk), Tier B (Moderate Risk), or Tier C (Low Risk) — assigned to each AI use case. See Section 10.

Section 7: Governance

7.1 Governance Roles and Responsibilities

Assign each governance function to an appropriate role. Consider establishing an AI Governance Committee or assigning AI governance responsibilities to an existing committee. Responsibilities may include reviewing AI tool performance, monitoring implementation, evaluating incidents and concerns, overseeing risk mitigation efforts, and recommending policy or operational changes when needed.

Appendix A

Governance Roles and Contacts: Enter individual names, contacts, and backup coverage here. Appendix A may be updated when personnel change without a formal policy revision.

CAH / Small Hospital Note

In smaller hospitals, governance responsibilities may be consolidated across leadership roles due to organizational structure, limited staffing capacity, and operational needs. A single individual may fulfill multiple governance functions. The Hospital should clearly document assigned responsibilities and identify appropriate backup coverage for critical governance functions in *Appendix A*.

Governance Function	Assigned Role / Title	Assigned Designee's Role/Title
Overall AI policy authority and final approval	*[e.g., CEO / President]*	
Day-to-day AI policy coordination	*[e.g., Chief Compliance Officer]*	
Clinical AI oversight and patient safety	*[e.g., Chief Medical Officer]*	
Nursing / care workflow AI oversight	*[e.g., Chief Nursing Officer]*	
Technical review and cybersecurity	*[e.g., IT Director / CISO]*	
Risk classification of AI tools	*[e.g., Compliance / IT]*	
Procurement and vendor management	*[e.g., Supply Chain / Procurement]*	
HIPAA and privacy compliance	*[e.g., Privacy Officer]*	
Workforce training oversight	*[e.g., HR / Education]*	
Public and patient communications on AI	*[e.g., Marketing / PR]*	
Ethics Hotline (anonymous reporting)	*[e.g., Third-party service]*	

7.2 Enforcement and Corrective Action

The Hospital will address non-compliance through (check all that apply):

- ☐ Verbal counseling and mandatory retraining
- ☐ Written warning in employee file
- ☐ Suspension of AI tool access privileges
- ☐ Medical staff peer review (for clinical staff violations, per Medical Staff Bylaws)
- ☐ Termination of employment or contract
- ☐ Other: _____

Violations should be reported to: _____ (Role / Title / Contact). Individuals who report violations in good faith are protected from retaliation under Hospital policy.

Section 8: Acceptable and Prohibited Use Overview

Core Principle: AI shall augment and not replace clinical judgment, professional accountability and patient-centered care.

8.1 AI May Be Used When It:

- ☐ Advances the Hospital's patient care mission and operational goals
- ☐ Has an assigned risk tier with appropriate controls (see Section 10)
- ☐ Has a completed BAA where PHI is involved, or an approved security review
- ☐ Operates under human oversight proportional to risk
- ☐ Complies with all requirements stated in this policy and with all applicable laws and regulation
- ☐ Is recorded in the AI Use Register (Appendix B)
- ☐ Staff using it have completed required training

8.2 AI Is Prohibited Without Specific Approval For:

- ☐ Autonomous clinical diagnosis, prescription or treatment orders without attending physician review and approval
- ☐ Processing PHI in tools not covered by a BAA approved by the Privacy Officer
- ☐ Automated patient triage or prioritization without real-time clinical oversight
- ☐ Publishing patient-facing communications or press releases without clinical and communications review
- ☐ Employment decisions without qualified HR / leadership oversight
- ☐ Entering patient records, billing information or employee records into publicly accessible or non-approved AI tools
- ☐ Other: _____

Section 9: AI Documentation and Notetaking Tools

Section 9.1 covers ambient clinical documentation scribes. Section 9.2 covers meeting AI notetakers. See Module A for full clinical documentation governance requirements if your hospital uses ambient scribes.

9.1 Approved Ambient Documentation Tools

Appendix E

Approved Tool Lists: List approved ambient documentation tools (name, vendor, CMO approval date, BAA status, oversight owner). Update when tools change — no policy revision required.

Requirements for clinical AI documentation tools (check all that apply):

- ☐ Tool must be covered under an active BAA reviewed by the Privacy Officer
- ☐ Physician or APP must review and attest all AI-generated documentation before it becomes part of the medical record
- ☐ Patients must be verbally informed before the tool is activated; declination must be honored and documented
- ☐ Audio or transcript data shall not be retained beyond the minimum operational period unless specifically approved by the Hospital and permitted under applicable law and Hospital policy.
- ☐ Tool must be tested for accuracy across patient populations, including non-English speakers
- ☐ Other: _____

Suggested Patient Disclosure Script (adapt as needed):

"I use an AI tool to help document our conversation so I can focus on you. The notes will be reviewed by me before they are added to your chart. You may decline this at any time."

9.2 Meeting and Administrative AI Notetakers

Requirements for meeting AI notetaking tools (check all that apply):

- ☐ AI notetaking tools may be used only when approved by the meeting lead
- ☐ All participants, including internal and external must be notified in advance
- ☐ AI notetakers shall not be used for meetings involving PHI, HR matters, peer review or internal investigations unless the tool has been approved at the appropriate security level and all applicable safeguards are in place
- ☐ AI-generated meeting notes are drafts and must be reviewed before distribution
- ☐ Other: _____

Section 10: Risk and Security Framework

Use this section to classify all AI tools and assign appropriate controls. Complete the Task-Tool Matrix (Section 10.6).

10.1 Tier A — High Risk / Clinical and Sensitive Use

Tier A: AI used in direct patient care, clinical decision-making, PHI processing or functions that could directly affect patient safety or legally protected rights.

Examples at this Hospital (check all that apply):

- ☐ AI-assisted diagnosis or clinical decision support affecting treatment
- ☐ Predictive models for deterioration, sepsis or readmission risk
- ☐ Radiology or pathology AI that flags or prioritizes results
- ☐ AI that supports prior authorization requests to payers
- ☐ AI used in financial assistance or presumptive Medicaid eligibility screening
- ☐ Other: _____

Minimum required controls — Tier A:

Data security / BAA review assigned to (role)	
Clinical validation before deployment — assigned to (role)	
Human-in-the-loop: licensed clinician reviews all outputs — assigned to (role)	
Incident notification within 24 hours — assigned to (role)	

10.2 Tier B — Moderate Risk / Operational Use

Tier B: AI supporting core operations — scheduling, revenue cycle, communications, reporting — where outputs may shape decisions but do not directly affect patient care.

Examples at this Hospital:

- ☐ AI-assisted revenue cycle tools
- ☐ AI used for staff scheduling, room utilization or operational capacity planning (no patient-level data)
- ☐ Chatbots handling general FAQs (hours, directions, billing questions) with no clinical content
- ☐ Translation AI for patient communications (non-clinical)
- ☐ Policy document drafting assistance
- ☐ AI-drafted patient satisfaction survey follow-ups
- ☐ Other: _____

Minimum required controls — Tier B:

QA review of AI outputs assigned to (role)	
Vendor privacy and security confirmation assigned to (role)	

10.3 Tier C — Low Risk / Internal / Administrative Use

Tier C: AI used for non-sensitive, internal tasks: brainstorming, drafting, summarizing public documents, learning.

Examples at this Hospital (add your own):

- ☐ Internal talking points or outline drafts using non-PHI content
- ☐ Summarizing publicly available policies or guidelines
- ☐ Grammar or readability review of non-sensitive documents
- ☐ Other: _____

Minimum controls: Staff must complete acceptable-use training. No PHI, personally identifiable information (PII) or confidential data. Treat outputs as drafts.

10.4 Reclassification Rule

If an AI tool's use expands to include PHI, clinical decisions or increased automation, it must be reclassified to the higher tier immediately and brought into full compliance before continued use.

10.5 Tool Security Levels

Level	Description	Minimum Controls
Level 1 — High Security	Processes PHI / PII; affects clinical decisions; involves regulated data.	BAA required; encryption at rest and in transit; multifactor authentication (MFA); HIPAA / SOC 2 compliance; human approval of all outputs; 24-hour incident notification
Level 2 — Medium Security	Supports operations; no direct patient care impact.	No PHI / PHII; vendor privacy confirmed; access controls; staff QA review; 24-hour incident notification
Level 3 — Low Security	Internal non-sensitive use only. No official outputs.	No PHI / PII; no-train option enabled if available; acceptable-use training; report accidental PHI entry immediately

10.6 Task–Tool Combination Matrix

For most hospitals: Tier A = Level 1 only. Tier B = Level 1 or 2. Tier C = any level (no PHI).

Task Risk/Tool Security	Level 1 (High Security)	Level 2 (Medium Security)	Level 3 (Low Security)
Tier A — High Risk	Allowed	Prohibited	Prohibited
Tier B — Moderate Risk	Allowed	Allowed	Prohibited
Tier C — Low Risk	Allowed	Allowed	Allowed

Hard Guardrail: *No AI task may operate at a lower security level than its actual risk requires.*

Section 11: Clinical Competency and Acceptable AI Use

11.1 Clinical Staff Requirements

Clinical staff using AI in patient care must (check all that apply):

- ☐ Possess the clinical competency and licensure to perform the underlying care task independently
- ☐ Understand how the AI tool works sufficiently to evaluate outputs and identify errors
- ☐ Complete required AI training before using any Tier A or Tier B tool
- ☐ Apply independent clinical judgment and not defer to AI output without critical review
- ☐ Document when and how AI informed a clinical decision, per EHR policy
- ☐ Use of only approved tools listed in the AI Use Register
- ☐ Other: _____

11.2 Restrictions for High-Risk Clinical Tasks

- ☐ AI shall be used for Tier A clinical tasks only by staff who can perform the underlying task independently.
- ☐ AI may not substitute for foundational clinical competency or independent professional judgment.
- ☐ Supervising physicians and preceptors are fully accountable for AI-assisted outputs produced by trainees under their supervision.
- ☐ Other: _____

Section 12: Training and Readiness Requirements

All Covered Persons must complete training before using any Hospital-approved AI tool. Training completion must be documented.

12.1 Required Training Topics

All Covered Persons must complete training covering (check all that apply):

- ☐ General AI literacy: capabilities, limitations and risks in health care
- ☐ HIPAA and data privacy in the context of AI tools
- ☐ Hospital AI policy requirements and acceptable use
- ☐ Recognizing and reporting AI errors, bias and incidents
- ☐ Clinical-specific training for each approved Tier A tool before first use
- ☐ Rural AI literacy: how AI-influenced decisions (e.g., triage, referral, risk scoring, benefit eligibility, care coordination) may interact differently with rural access barriers such as distance to services, transportation and broadband limitations
- ☐ Other: _____

12.2 Training Completion and Acknowledgment

- [ ] Learning Management System (LMS) record
- [ ] Electronic attestation form
- [ ] Signed paper acknowledgment (use the Staff Acknowledgment Form at the end of this policy)

Training records maintained by (department / role)	

12.3 Tier A Tools — Additional Requirement

Staff must complete training AND obtain prior written approval before using any Tier A AI tool.

Written approval authority for Tier A tool use (role)	

12.4 Refresher Training Triggers

Refresher training is required when (check all that apply):

- [ ] A new AI tool is deployed or an existing tool undergoes a major update
- [ ] Applicable law or regulation changes
- [ ] An AI-related incident, error or bias event is identified
- [ ] Annual policy review identifies training gaps
- [ ] Other:

Section 13: Misuse of AI

13.1 Prohibited Personnel Conduct

The following conduct is prohibited and may result in disciplinary action up to and including termination:

- ☐ Creating, sharing or amplifying false or AI-generated misinformation about patients, staff or the Hospital
- ☐ Using AI to impersonate a physician, clinician or Hospital official
- ☐ Entering PHI, employee records or confidential data into unapproved or consumer AI tools
- ☐ Bypassing procurement, IT security or BAA review requirements to use an unauthorized AI tool
- ☐ Using Hospital AI systems for personal projects or non-official activities
- ☐ Using AI to harass, discriminate against or intimidate any patient, visitor or staff member

Report violations to (role / title)	

Individuals who report violations in good faith are protected from retaliation under Hospital policy.

Section 14: Vendor and Third-Party Obligations

14.1 BAA and Contractual Requirements

All AI vendors handling PHI must (check all that apply):

- ☐ Execute a valid HIPAA Business Associate Agreement (BAA) before any PHI is shared or processed
- ☐ Comply with this policy and all applicable HIPAA Privacy and Security Rule requirements
- ☐ Notify the Hospital of any breach, security incident or AI system failure within 24 hours
- ☐ Permit the Hospital to audit AI tool performance and data handling on reasonable notice
- ☐ Do not use Hospital data to train or improve AI models without prior written Hospital authorization
- ☐ Other: _____

14.2 Contract Language

Sample Language: AI Use Contract Clause — include in all AI vendor contracts:

"The Vendor acknowledges that [Hospital Name] has adopted an Artificial Intelligence (AI) Use Policy governing the responsible and ethical use of AI. Any use of AI tools, models, platforms or services in connection with services provided under this agreement shall comply with that policy, all applicable HIPAA requirements, and relevant federal and state law. Vendor shall promptly notify the Hospital of any material changes to its AI systems, data handling practices or security posture prior to implementation of such changes."

14.3 Transition Period for Existing Contracts

Standard transition period (e.g., six months)	
Extended transition period by written request (e.g., 12 months)	
Title of staff member who reviews extension requests	

All new contracts signed after this policy's effective date must comply immediately.

Section 15: Responsible Use, Safeguards and Transparency

15.1 Human Oversight Requirements

The Hospital requires (check all that apply):

- ☐ All AI systems must operate under meaningful human oversight — AI outputs inform but do not replace judgment
- ☐ Clinicians must review and validate AI-assisted findings before they affect patient care
- ☐ Tier A AI tools require documented review and approval before deployment
- ☐ Significant or recurring AI issues must be reviewed by a governance body, such as an AI Governance Committee
- ☐ Staff must escalate AI output errors or safety concerns per the escalation process below

Escalation contact / process for AI errors (e.g., charge nurse, then CMO)	

15.2 Bias Mitigation

The Hospital requires (check all that apply):

- ☐ Proactive bias assessment before deploying any Tier A tool, documented in the AI Use Register
- ☐ Vendors to disclose known limitations and populations where performance may be lower
- ☐ Semi-annual review of AI-assisted outcomes for disparate impacts, reported to CMO
- ☐ Staff training to include guidance on recognizing and addressing AI bias
- ☐ Semi-annual review of AI-assisted outcomes includes geography and service area alongside race, ethnicity, age and other bias dimensions, with particular attention to rural, low-volume or critical-access patient populations
- ☐ Other: _____

15.3 Transparency to Patients and Staff

The Hospital's transparency commitments include (check all that apply):

- ☐ Patients will be informed when AI materially influences a diagnosis, treatment recommendation or care decision
- ☐ Hospital maintains an AI Use Register (*Appendix B*) accessible to authorized staff
- ☐ A public-facing summary of Hospital AI use will be available on the Hospital website
- ☐ Staff will receive regular updates on approved AI tools and policy changes
- ☐ Significant AI incidents involving patient harm will be disclosed per Hospital incident policy

15.4 Tier A Documentation Requirements

Appendix B

Approved Tool Lists: Document each Tier A tool's clinical purpose, PHI status, BAA reference, safeguards, human review process and final decision authority there. The AI Use Register (*Appendix B*) serves as the primary living inventory.

Sample documentation statement for the medical record (adapt for each tool):

"AI was used to support [task, e.g., sepsis risk flagging] by [AI role, e.g., generating a risk score]. The clinical decision to [action taken] was made independently by the attending physician based on full clinical assessment. The AI output was one input among several considered."

Section 16: Acquisition of AI Tools and Systems

16.1 Pre-Procurement Requirements

No AI tool may be purchased, piloted or deployed without completing the Hospital's AI Tool Review Process.

Before acquiring any AI tool, the requesting department must submit a written request describing:

- ☐ Clinical or operational purpose and expected benefit
- ☐ Proposed risk tier and security level
- ☐ Data involved, including whether PHI is processed
- ☐ BAA status and vendor HIPAA compliance documentation
- ☐ Integration requirements with the EHR or existing systems
- ☐ Clinical validation evidence (required for Tier A tools)

Tier A tool requests require written approval from all of the following:

Clinical sign-off (role)	
IT / Security sign-off (role)	
Compliance / Privacy sign-off (role)	
Final approving authority (role)	

16.2 AI Use Register

The AI Use Register is maintained in Appendix B and may be updated by the designated role when tools are added, retired or reclassified without a formal policy revision. Any update must be communicated to the Policy Owner within five (5) business days.

16.3 Procurement Preferences

The Hospital prefers AI tools with (check all that apply):

- ☐ Explainability features
- ☐ ADA / Section 508 compliance
- ☐ Human-in-the-loop capabilities by design
- ☐ Performance data across diverse patient populations
- ☐ Data minimization and no-train options
- ☐ EHR integration without data duplication risk
- ☐ Vendor disclosure of how the tool performs in rural, low-volume or low-connectivity settings, including known limitations and plain-language documentation of conditions under which performance may vary

16.4 Decommissioning

When an AI tool is retired, confirm:

- ☐ All PHI reviewed for archival, transfer or destruction per HIPAA and the Records Retention Policy
- ☐ AI Use Register updated to mark the tool as retired
- ☐ Staff notified to cease use

Section 17: Incident Response and Occurrence Reporting

Fill in your occurrence reporting system name and responsible party contacts in the shaded cells.

Appendix A

Responsible party contacts (CNO, IT Director, Privacy Officer, CCO, Ethics Hotline) are maintained in Appendix A — Governance Roles and Contacts. Update Appendix A when contacts change; no policy revision is required.

Any Covered Person who identifies an AI-related error, patient safety concern, suspected HIPAA breach or policy violation must take the following steps:

Event Type	Required Action	Responsible Party — Fill In
Clinical AI event with potential patient harm (Tier A)	File occurrence report in [occurrence system] immediately. Notify charge nurse and attending nurse. CNO notification within one (1) hour.	Charge nurse (CNO):
Suspected HIPAA breach or unauthorized PHI disclosure	Notify IT Director and Privacy Officer within 24 hours. Privacy Officer initiates HIPAA Breach Assessment per [Breach Notification Policy #].	IT Director: Privacy Officer:
Cybersecurity incident (unauthorized access, ransomware)	Notify IT Director immediately. Follow [Cybersecurity Incident Response Plan #].	IT Director:
Policy violation or personnel misuse	Report to direct supervisor and CCO. CCO determines corrective action within 10 business days.	CCO: Ethics Hotline:

Section 18: Patient Rights and AI Disclosure

Patients have the right to be informed when AI materially influences a diagnosis, treatment recommendation, care plan, or clinical decision affecting their care. The Hospital's patient rights commitments regarding AI include (check all that apply):

- ☐ Patients are informed when AI materially influences their care decisions
- ☐ Patients may request a plain-language explanation of how AI was used in their care
- ☐ Patients may decline AI-assisted documentation (governed by Module A if selected)
- ☐ Patient rights related to AI are incorporated into the Patient Rights and Responsibilities Policy — policy number: _____
- ☐ Other: _____

Section 19: Policy Review and Effective Date

19.1 Review Cycle

This policy shall be reviewed (check one):

- ☐ Annually — recommended for most hospitals
- ☐ When there are significant changes to AI technologies, applicable laws or regulations, organizational operations, or AI use cases
- ☐ Every two years
- ☐ When the hospital's patient population or service area changes meaningfully (e.g., new rural service line, new telehealth partnership, expanded catchment area)
- ☐ Other: _____

19.2 Policy Approval Signatures

Approved by (CEO / Name / Signature)	Title
Date	**Policy Number**
Clinical Review — CMO (Name / Signature)	**Compliance Review — CCO (Name / Signature)**
IT / Security Review (Name / Signature)	**Board Ratification (Chair / Date)**

19.3 Staff Acknowledgement Form

This form may be reproduced separately or distributed electronically. Completed forms are retained by HR / Education.

I have read and understand the Hospital's Artificial Intelligence (AI) Use Policy. I agree to comply with all provisions. I understand that violations may result in disciplinary action up to and including termination.

Printed Name	Job Title / Department	Signature	Date Signed

19.4 Record of Revisions

Revision #	Section(s) Revised	Date	Description of Change

Part 2

Add-On Modules

Include only the modules that match your hospital's AI tool inventory.

Each module is self-contained and slots in after Section 19.

ADD-ON MODULE A:
Ambient Documentation AI

Include if your hospital uses any AI scribe, ambient listening tool, or AI that generates content entered into the EHR medical record.

Which hospitals need this module?

- ✓ You use Nuance DAX, Abridge, Suki or a similar ambient documentation tool
- ✓ Your EHR vendor (e.g., Epic) has enabled an ambient note-generation feature
- ✓ Any AI generates draft clinical notes that are then reviewed and filed by clinicians

A.1 Clinician Attestation and Medical Record Finalization

AI-generated clinical documentation, including notes, summaries and structured data produced by ambient scribes or clinical decision support platforms constitutes a draft only until reviewed and electronically signed by the responsible clinician. The signing clinician assumes full professional and legal accountability for the content of the finalized record. No AI-generated note may be filed in the medical record without clinician review and attestation.

A.2 Required Patient Disclosure

When using any Hospital-approved ambient documentation tool, clinical staff must provide an approved verbal disclosure to the patient at the beginning of the encounter. Approved disclosure scripts for each authorized tool are maintained in Appendix C. No ambient tool may be used without an approved script in Appendix C. Patient declination must be documented in the EHR. No adverse inference may be drawn from a patient's decision to decline.

Bias Check: Before you obtain patient consent make sure to check with your tool vendor to see if the tool has been assessed for accuracy across regional accents, dialects and speech patterns common to this Hospital's service area, not only across languages.

A.3 Governance and Oversight

CMO-designated clinical lead for ambient documentation oversight	

Appendix E

Approved Tool Lists, Module A: List approved ambient documentation tools there. Update when tools change without a policy revision.

Oversight requirements:

- ☐ CMO must approve each ambient documentation tool before clinical deployment
- ☐ Patient declination documented in EHR using standard notation
- ☐ Audio or transcript data not retained beyond session without written authorization
- ☐ Tool tested for accuracy across patient populations, including non-English speakers
- ☐ Tool has a defined fallback procedure (e.g., manual documentation) for use during connectivity interruptions, and clinical staff are trained on it
- ☐ Other:

A.4 Medical Staff Credentialing and AI Privileging

The Hospital's approach to Medical Staff oversight of clinical AI documentation includes (check all that apply):

- ☐ The Medical Executive Committee (MEC) reviews and approves all Tier A ambient documentation tools before deployment
- ☐ Use of specific high-risk documentation AI tools requires a specific clinical privilege in Medical Staff Bylaws or credentialing criteria
- ☐ AI-related adverse events involving licensed practitioners are referred to the peer review process per Medical Staff Bylaws
- ☐ Other:

MEC review / approval process reference (Bylaw section or policy number)	

ADD-ON MODULE B
Diagnostic and Radiology AI

Include if your hospital uses AI that reads, flags, triages or prioritizes imaging, pathology or laboratory results.

Which hospitals need this module?

- ✓ A radiology AI tool prioritizes or flags imaging results before radiologist review
- ✓ AI assists in reading or interpreting pathology slides or lab values
- ✓ Any AI generates diagnostic outputs that inform clinical decisions

B.1 Clinical Validation Requirements

Before any diagnostic or radiology AI tool is deployed in a clinical setting, the CMO must complete a written validation review documenting:

- ☐ Available vendor evidence of the tool's training data and performance characteristics
- ☐ Known performance limitations and populations where performance may be reduced
- ☐ Results of any local validation or pilot testing
- ☐ Bias assessment across race, ethnicity, gender, age and patient populations served by this Hospital
- ☐ Vendor evidence of the tool's validation, or lack of validation, on rural, low-volume or critical-access populations comparable to this Hospital's service area
- ☐ Assessment of whether lower historical utilization in this Hospital's service area reflects access barriers rather than lower clinical need, where relevant to the tool's function
- ☐ Other: _____

Validation review assigned to (role)	

B.2 Human Oversight Requirements

The following human oversight requirements apply to all diagnostic and radiology AI tools at this Hospital:

- ☐ All AI-generated diagnostic outputs (flagging, prioritization, reads) must be reviewed and validated by a qualified, licensed clinician before influencing patient care
- ☐ Radiologist or pathologist of record retains full professional and legal accountability for all finalized diagnostic interpretations
- ☐ AI outputs may not be used to delay or override clinical judgment
- ☐ Other: _____

B.3 Approved Diagnostic AI Tools

Appendix B and E

Approved Tool Lists, Module B: List approved diagnostic and radiology AI tools (tool / vendor, diagnostic function, BAA status, CMO validation date, oversight owner) there.

B.4 Medical Staff Oversight

- ☐ MEC reviews and approves all Tier A diagnostic AI tools before deployment
- ☐ Use of AI-assisted autonomous image reading requires a specific clinical privilege in Medical Staff Bylaws
- ☐ AI-related adverse diagnostic events are referred to the peer review process per Medical Staff Bylaws
- ☐ Other: _____

MEC review / approval process (Bylaw section or policy number)	

ADD-ON MODULE C

Predictive Alerts and Clinical Decision Support

Include if your hospital uses AI that generates clinical alerts, risk scores or flags delivered to nursing or physician workflows.

Which hospitals need this module?

- ✓ Your EHR has an active sepsis prediction model, deterioration index or readmission risk flag
- ✓ AI-generated alerts appear in nursing or physician workflows
- ✓ Any AI tool scores or prioritizes patients for clinical action

C.1 Alert Fatigue and Clinical Safety

The CMO and CNO are jointly responsible for monitoring the clinical impact of AI-generated alerts. The Hospital will (check all that apply):

- ☐ Review AI-generated alert volume and clinical response rates at least semi-annually
- ☐ Convene a CMO-led review if alert volume is found to contribute to alarm fatigue or patient safety concerns
- ☐ Require CMO approval for any changes to AI alert thresholds or sensitivity settings in the EHR
- ☐ Escalate recurring alert fatigue findings to the Patient Safety and Quality Committee
- ☐ Ensure that alert response review accounts for this Hospital's available clinical staffing levels, particularly during off-hours or night shifts, where the tool's design assumptions about response capacity may not reflect this Hospital's actual staffing
- ☐ Other: _____

C.2 Approved Predictive Alert Tools

Alert threshold review assigned to (role)	

Appendix E

Approved Tool Lists, Module C: Full predictive alert tool inventory (tool / vendor, alert type, BAA status, alert response owner, last threshold review) is maintained there.

C.3 CDS Human Override Requirements

For all clinical decision support AI at this Hospital (check all that apply):

- ☐ Clinicians may override any AI-generated alert or recommendation without penalty and without requiring documentation of the reason
- ☐ Override patterns are reviewed periodically by the CMO to identify potential patient safety trends
- ☐ AI-generated risk scores are one clinical input among several and shall never be treated as a stand-alone clinical determination
- ☐ Other: _____

C.4 Incident Reporting for Alert-Related Events

Any clinical AI event in which an AI-generated alert may have contributed to patient harm — or in which failure to act on an alert contributed to patient harm — must be filed in the Hospital's occurrence reporting system immediately.

Occurrence reporting system name	

CNO notification contact for Tier A alert events	

ADD-ON MODULE D
Revenue Cycle AI

Include if your hospital uses AI for coding, prior authorization, claims editing, or any function affecting Medicare or Medicaid billing.

Which hospitals need this module?

- ✓ An AI tool assists with coding, code review, or claims editing before submission
- ✓ AI supports prior authorization requests to payers
- ✓ Any revenue cycle function affecting Medicare or Medicaid billing uses AI

False Claims Act risk: AI-assisted coding errors can constitute false claims under federal law.

A qualified coder or clinician must review and approve all AI-generated codes before submission. AI-suggested codes may not be submitted to Medicare or Medicaid without human review, regardless of the tool's confidence level.

D.1 Revenue Cycle AI Requirements

The Hospital's requirements for AI used in revenue cycle functions include (check all that apply):

- ☐ A qualified coder or clinician reviews and approves all AI-generated codes before claims submission
- ☐ AI-assisted prior authorization tools are used for support only; final authorization decisions comply with payer contracts and CMS requirements
- ☐ Revenue cycle AI tools are included in the Hospital's Compliance Program audit schedule
- ☐ Vendors providing revenue cycle AI must attest in writing that their tools comply with applicable CMS billing rules and OIG guidance
- ☐ AI-identified upcoding, undercoding, or unusual billing patterns are reviewed by the CCO and reported through the Compliance Program
- ☐ AI-assisted prior authorization and claims tools are monitored for disproportionate denial or delay patterns affecting patients with limited access to alternate providers or extended travel distances
- ☐ Other: _____

D.2 Approved Revenue Cycle AI Tools

Appendix E

Approved Tool Lists, Module D: List approved revenue cycle AI tools (tool / vendor, function, BAA status, coder / clinician review process, oversight owner) there.

D.3 Board Oversight

The Board of Trustees will receive (check all that apply):

- ☐ An annual AI governance report summarizing approved tools, incidents, training compliance, and policy updates
- ☐ Notification of any significant AI-related patient safety event or HIPAA breach involving an AI system
- ☐ Ratification of this AI Use Policy and any major revisions
- ☐ A summary of AI-related compliance findings from the Compliance Program audit schedule
- ☐ Other: _____

Annual AI report presented by (role)	
Frequency / Board meeting (e.g., Annual — January)	

ADD-ON MODULE E

Generative AI and Productivity Tools

Include if staff use ChatGPT, Microsoft Copilot, Google Gemini, or similar tools for drafting, summarizing, or administrative productivity.

Which hospitals need this module?

- ✓ Any staff member uses ChatGPT, Copilot, Gemini, or similar tools for work purposes
- ✓ Your hospital has licensed Microsoft Copilot for M365 or a similar enterprise GenAI tool
- ✓ You want explicit policy coverage for consumer AI tools staff may use on personal devices

E.1 Authorized Use of Generative AI

The Hospital's authorized use of generative AI tools is governed by the risk tier framework in Section 10. Generative AI tools may be used only when:

- ☐ The tool appears in the AI Use Register (Appendix B) with an assigned tier and security level
- ☐ For Tier B tools: the tool has been procured by the Hospital with a Data Processing Agreement or BAA where PHI may be involved
- ☐ For Tier C tools: the tool is used for internal, non-sensitive, non-PHI tasks only, and outputs are treated as informal drafts
- ☐ Staff have completed required AI training before first use
- ☐ Other: _____

E.2 Prohibited Generative AI Use

Generative AI tools may not be used for (check all that apply):

- ☐ Entering PHI, employee records, financial data, or other confidential Hospital information into any publicly accessible or non-BAA-covered AI tool
- ☐ Creating, publishing, or distributing AI-generated content that misrepresents the Hospital or its staff
- ☐ Generating deepfakes, synthetic media, or any content that impersonates a clinician, patient, or Hospital official
- ☐ Substituting AI-generated responses for qualified clinical advice in any patient-facing context
- ☐ Other: _____

A staff member's personal paid subscription (e.g., personal ChatGPT Plus, Claude Pro) is classified as Level 3 — even if the employee pays for it.

These tools have not been procured by the Hospital, carry no Hospital data protections, and may only be used for Tier C tasks with no PHI or PII.

If your hospital prohibits personal AI tools for all work-related tasks, you may use this language:

Personal AI subscriptions (e.g., ChatGPT Plus, Claude Pro, Microsoft Copilot) may not be used for any work-related task, regardless of task sensitivity or data type. Only tools procured and approved by [Hospital Name] are authorized for use in connection with Hospital business.

E.3 Approved Generative AI Tools

Appendix E

Approved Tool Lists, Module E: List approved generative AI tools (tool / vendor, authorized use cases, tier, security level, BAA and Data Processing Agreement (DPA) status, oversight owner) there.

E.4 AI-Generated Content Review Requirements

Content requirements for AI-generated outputs (check all that apply):

- ☐ All AI-generated content used in official communications, patient education, or public-facing materials must be reviewed and approved by a qualified staff member before publication
- ☐ Staff must not submit AI-generated clinical documentation, reports, or analyses without review and personal attestation
- ☐ AI-generated content must not be represented as the original work of a specific individual without disclosure
- ☐ AI-generated patient-facing communications (e.g., portal messages, chatbots, automated outreach) do not assume reliable broadband, smartphone access or digital literacy and a non-digital alternative, such as phone calls and mailed letters, remains available and is not treated as a lesser fallback
- ☐ Other: _____

Appendix A

Governance Roles and Contacts

This appendix may be updated when personnel change without requiring a formal policy revision. Communicate all updates to the Policy Owner within five (5) business days.

Appendix Version Date	Last Revised By

Governance Function	Suggested Role	Assigned Name / Title	Contact	Assigned Designee Name / Title	Contact
Overall AI policy authority and final approval	CEO / President				
Day-to-day AI policy coordination	Chief Compliance Officer				
Clinical AI oversight and patient safety	Chief Medical Officer				
Nursing / care workflow AI oversight	Chief Nursing Officer				
Technical review and cybersecurity	IT Director / CISO				
Risk classification of AI tools	Compliance / IT Director				
Procurement and vendor management	Supply Chain / Procurement				
HIPAA and privacy compliance	Privacy Officer				
Workforce training oversight	HR / Education Director				
Public / patient communications on AI	Marketing / Communications				
Ethics Hotline (anonymous reporting)	Third-party service				
Rural / community AI liaison	Community Benefit / Rural Health Program Lead				
Additional role (as needed)					

Appendix B

AI Use Register

Maintained by the IT Director. Update when tools are added, retired or reclassified. Communicate updates to the Policy Owner within five (5) business days. No tool may be used unless it appears in this Register.

Last Revised By

Tool / Vendor	Purpose	Risk Tier	Security Level	Rural / Low-Volume Validation Status:	Known Limitations Documented (Y/N)	BAA / Agreement Status and Reference Number	Oversight Owner	Date Approved	Date Last Reviewed

Appendix C

Approved Patient Disclosure Scripts

Maintained by the CMO. Update when new ambient documentation tools are approved or disclosure language changes. No ambient tool may be used without an approved script here.

Where a hospital serves patients who travel significant distances or face limited follow-up access, disclosure scripts should also make clear that declining an AI tool does not delay, reduce or otherwise change the care they receive that visit. This reduces the risk that patients with fewer opportunities to return will decline an AI-assisted tool out of concern it is required to receive care.

Appendix Version Date	Last Revised By

C.1 Disclosure Script — Tool 1

Approved Disclosure Script

Include if your hospital uses AI for coding, prior authorization, claims editing, or any function affecting Medicare or Medicaid billing.

Applicable Tool Name	CMO Approval Date

Approved Script Text (enter verbatim approved language below):

Sample: “I use an AI tool to help document our conversation so I can focus on you. The notes will be reviewed and approved by me before entering your chart. You may decline at any time — simply let me know.”

Standard EHR declination notation: “Patient declined AI-assisted documentation. Visit documented manually per patient request.”

C.2 Script Inventory

Tool Name	CMO Approval Date	Last Revised	Notes

Appendix D

Regulatory References and Internal Policy Cross-References

Complete the Hospital Policy Number column with your internal policy numbers. Update when policy numbers change without requiring a formal policy revision.

Appendix Version Date	Last Revised By

Document / Standard	Regulatory Citation	Hospital Policy Number
HIPAA Privacy Rule	45 C.F.R. Parts 160 and 164	
HIPAA Security Rule	45 C.F.R. Part 164, Subparts A and C	
Joint Commission (LD, IM, NPSG Standards)	TJC Comprehensive Accreditation Manual	
CMS Conditions of Participation	42 C.F.R. Part 482	
HIPAA Privacy Policy (internal)		
Information Security Policy (internal)		
EHR Governance Policy (internal)		
Breach Notification Policy (internal)		
Cybersecurity Incident Response Plan (internal)		
Patient Rights and Responsibilities Policy (internal)		
Medical Staff Bylaws		
Non-Retaliation Policy (internal)		
Records Retention Policy (internal)		
Rural proofing considerations (Federation of American Scientists (FAS) / National Rural Health Association (NRHA) guidance)	Non-binding practice guidance, not a regulatory requirement	N/A, reference only
[Add additional policy]		
[Add additional policy]		

Appendix E

Approved Tool Lists by Module

Complete only the sections for modules your hospital has selected.

Update when tools are added, retired, or changed — no formal policy revision required.

Communicate all updates to the Policy Owner within five (5) business days.

All tools must also appear in the AI Use Register (Appendix B).

Last Revised By

E-A Module A: Approved Ambient Documentation Tools

List all ambient documentation tools approved for clinical use at this Hospital.

Tool / Vendor	Clinical Use Description	BAA Status	Rural / Low-Volume Validation Status:	Oversight Owner

E-A.1 Tier A Documentation — Safeguards and Human Review

For each Tier A ambient documentation tool, document clinical purpose, PHI status, safeguards, and final decision authority.

AI Tool / System	Clinical Purpose	PHI Involved? (Yes/No — if Yes, BAA reference.)	Rural / Low-Volume Validation Status:	Safeguards and Human Review Process	Final Decision Authority

Sample documentation statement for the medical record (adapt for each tool):

"AI was used to support [task, e.g., sepsis risk flagging] by [AI role, e.g., generating a risk score]. The clinical decision to [action taken] was made independently by the attending physician based on full clinical assessment. The AI output was one input among several considered."

E-B Module B: Approved Diagnostic and Radiology AI Tools

List all diagnostic and radiology AI tools approved for clinical use at this Hospital.

Tool / Vendor	Diagnostic Function	BAA Status	Rural / Low-Volume Validation Status:	CMO Validation Date	Oversight Owner

E-C Module C: Approved Predictive Alert and CDS Tools

List all predictive alert and clinical decision support tools approved for use at this Hospital.

Tool / Vendor	Clinical Alert Type	BAA Status	Rural / Low-Volume Validation Status:	Alert Response Owner	Last Threshold Review

Assign alert threshold review role and list active alert tools:

AI tools generating clinical alerts at this Hospital (list)	
Alert threshold review assigned to (role)	

E-D Module D: Approved Revenue Cycle AI Tools

List all revenue cycle AI tools approved for use at this Hospital.

Tool / Vendor	Function (coding / prior authorization / claims)	BAA Status	Rural / Low-Volume Validation Status:	Coder/Clinician Review Process	Oversight Owner

E-E Module E: Approved Generative AI and Productivity Tools

List all generative AI tools approved for use at this Hospital.

Tool / Vendor	Authorized Use Cases	Tier	Security Level	BAA / DPA Status	Rural / Low-Volume Validation Status:	Oversight Owner

Appendix F

Control Role Assignments

Update when roles or personnel change — no formal policy revision required.

Communicate all updates to the Policy Owner within five (5) business days.

These assignments correspond to the minimum required controls in Section 10.

Appendix Version Date	Last Revised By

Tier A — High Risk: Required Control Role Assignments

Assign the responsible role for each required Tier A control.

Required Control	Key Staff Assigned Role/Title/Name	Backup/Designee Assigned Role/Title/Name
Data security / BAA review assigned to (role)		
Clinical validation before deployment — assigned to (role)		
Human-in-the-loop: licensed clinician reviews all outputs — assigned to (role)		
Incident notification within 24 hours — assigned to (role)		
Rural/low-volume validation disclosure review, confirming vendor-provided validation data (or documented absence of it) is on file before Tier A deployment — assigned to (role)		

Tier B — Moderate Risk: Required Control Role Assignments

Assign the responsible role for each required Tier B control.

QA review of AI outputs assigned to (role/title/name)	
Vendor privacy and security confirmation assigned to (role/ title / name)	


KANSAS HEALTH INSTITUTE
Informing Policy. Improving Health.


HEALTH
WORKS
KANSAS HOSPITAL
ASSOCIATION