September 2026

# AI Use Policy Template for Health Departments

*Includes Rural Proofing Additions*

PHIG PARTNERS
SHAPING TOMORROW'S PUBLIC HEALTH TODAY.

KANSAS HEALTH INSTITUTE
*Informing Policy. Improving Health.*

KHI/26-91

## Legal Disclaimer

This 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. Health departments should consult their own legal and other advisors before adopting or implementing an artificial intelligence use policy and should adapt this template to meet the needs of their individual organization.

Because AI technologies, regulations and best practices continue to evolve, health departments 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 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.

This work is supported by funds made available from the Centers for Disease Control and Prevention (CDC) of the U.S. Department of Health and Human Services (HHS), National Center for STLT Public Health Infrastructure and Workforce, through OE22-2203: Strengthening U.S. Public Health Infrastructure, Workforce, and Data Systems grant. 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.

# About This Resource

The *AI Use Policy Template for Health Departments* (hereafter, the *AI Use Policy Template*) provides health departments with a ready-to-complete artificial intelligence (AI) use policy organized into clearly labeled sections with checkboxes and fillable fields. It guides departments 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, 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. It is intended as a starting point and should be adapted to reflect your department's specific context, needs and applicable laws.

This *AI Use Policy Template* is accompanied by the *Companion to the AI Use Policy Template for Health Departments* (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 template and guide are designed to support local and state health departments 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 health departments to incorporate their own rural conditions directly into their AI use policy.


## Acknowledgments

The *AI Use Policy Template* and accompanying *Companion Guide* were developed by the Kansas Health Institute (KHI). The content was informed by *Developing Artificial Intelligence (AI) Policies for Public Health Organizations: A Template and Guidance*. It also draws on KHI's direct work with public health departments developing AI policies and governance approaches, including work with the Guam Department of Health and Social Services. These resources were also developed in response to a request from the Colorado Association of Local Public Health Officials (CALPHO) and informed by feedback from local public health agencies across Colorado. Portions of the structure and formatting were adapted from data governance policy and instruction guide materials developed by Flourish and Thrive Labs.

This work is supported by funds made available from the Centers for Disease Control and Prevention (CDC) of the U.S. Department of Health and Human Services (HHS), National Center for STLT Public Health Infrastructure and Workforce, through OE22-2203: Strengthening U.S. Public Health.



## Authors

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

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

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

KANSAS HEALTH INSTITUTE
*Informing Policy. Improving Health.*

## [Department / Agency Name]

| | |
|---|---|
| **Policy Title** | |
| **Policy Number** | |
| **Version** | |
| **Approving Authority** | |
| **Effective Date** | |
| **Next Review Date** | |

# 1: Purpose

*Purpose Statement (do not include this header in the policy; listed here for guide alignment)*

This policy establishes requirements and standards for the responsible and ethical use of artificial intelligence (AI) within _____ (the "Department"). It provides a framework to guide AI use across the Department, ensuring that when AI is used, it is implemented in ways that:

- ☐ builds and maintains public trust
- ☐ serves all communities equitably
- ☐ advances operational efficiency
- ☐ supports responsible innovation
- ☐ safeguards equitable access and outcomes
- ☐ for rural, frontier and geographically isolated communities
- ☐ Other: _____

while upholding the principles of:

- ☐ transparency
- ☐ accountability
- ☐ human oversight
- ☐ data privacy
- ☐ security
- ☐ workforce support
- ☐ Other: _____

# 2: Scope

This policy covers the following types of AI technologies used within the Department (check all that apply):

- ☐ AI tools, platforms and applications
- ☐ AI services and AI-enabled features embedded in other technologies
- ☐ Generative AI applications (e.g., tools that produce text, images, audio or code)
- ☐ AI systems that generate predictions, recommendations or decisions
- ☐ Agentic AI systems that can take actions, such as sending communications, entering or modifying records, retrieving data, scheduling or triggering workflows (see Section 17)
- ☐ Other _____

# 3: Applicability

This policy applies to (check all that apply):

- [ ] All divisions involved in procurement, development, deployment or management of AI
- [ ] All divisions that use AI technologies in operations or service delivery
- [ ] All divisions that use data outputs generated by AI models or systems
- [ ] Other _____

## 3.2. Staff and Third Parties

This policy applies to (check all that apply):

- [ ] All permanent / classified staff
- [ ] Limited term, temporary and unclassified staff
- [ ] Interns, fellows and practicum students
- [ ] Emergency/surge workforce (e.g., Medical Reserve Corps, outbreak-response hires)
- [ ] Governing board members / appointed commissioners
- [ ] Volunteers
- [ ] Contractors and consultants
- [ ] Grant-funded or partner-embedded staff working on-site
- [ ] Staff shared across jurisdictions or regional service agreements
- [ ] Other individuals or external organizations performing work on behalf of the Department:

_____

*Note: This section covers individuals performing work on behalf of the Department. It does not govern AI use by external partner agencies, data-sharing partners, or sister organizations. That should be addressed through data sharing agreements or vendor/Business Associate Agreement (BAA) contract language.*

## 3.3. Vendors

Selected vendors, including technology providers and software or cloud service providers may not directly subject to this policy but are governed through procurement requirements, contract terms and vendor assessments.

Third-party obligations, disclosure requirements, transition timelines and enforcement procedures are outlined in Section 14.

# 4: Alignment With Existing Policies (and Order of Precedence)

Check all relevant policies:

- [ ] HIPAA Privacy and Security Rules (45 CFR Parts 160 and 164)
- [ ] Family Educational Rights and Privacy Act (FERPA)
- [ ] Applicable federal laws and regulations
- [ ] Applicable federal and state executive orders on AI use
- [ ] State-specific laws and regulations (e.g., Colorado Open Records Act [CORA])
- [ ] Information security/cybersecurity policy
- [ ] Records retention policy and destruction policy
- [ ] Procurement policy / vendor management policy
- [ ] Applicable federal, state, tribal, territorial and local administrative rules and regulations
- [ ] Other: _____

# 5: Guiding Principles

The Department is committed to using AI in a way that is safe and aligned with its mission. The following principles guide all AI use by the Department and all covered third parties. *Check all principles the Department adopts:*

- ☐ **Human Oversight:** AI systems shall always be used with meaningful human oversight and judgment. Staff remains accountable for decisions informed by AI.
- ☐ **Bias Awareness and Mitigation:** The Department 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 reflect rural populations and documenting known limitations where such validation is unavailable.
- ☐ **Transparency:** The Department will be open with the public and stakeholders about when and how AI is used in operations.
- ☐ **Data Privacy:** The Department will safeguard the privacy and confidentiality of all data used in or provided to AI systems.
- ☐ **Data Security:** The Department is committed to protecting AI systems and data from unauthorized access, misuse and security breaches.
- ☐ **Environmental Responsibility:** When information is available, the Department will consider environmental impacts and energy use in AI procurement and deployment.
- ☐ **Innovation and Risk Management:** The Department will foster responsible innovation, leveraging AI carefully while monitoring risks.
- ☐ **Workforce Sustainability:** The Department will use AI to enhance capacity and reduce administrative burden, while ensuring AI does not replace essential staff roles or professional judgment.
- ☐ **Other:** _____

# 6: Key Definitions

| Term | Definition |
|---|---|
| **Artificial Intelligence (AI)** | Computer-based systems capable of performing tasks that typically require human intelligence, such as reasoning, learning, problem-solving, pattern recognition, perception or language understanding. |
| **Generative AI (GenAI)** | A subset of AI technologies that can create new content such as text, images, audio, video or code based on user input or other data. |
| **AI Tools** | Publicly accessible or procured AI platforms, applications or services used to generate content, analyze data, detect patterns or make predictions. |
| **AI System** | A machine-based system that generates outputs — such as predictions, content, recommendations or decisions — that can influence real or virtual environments. |

| Term | Definition |
|---|---|
| **Agentic AI** | An AI system that plans and carries out multi-step tasks toward an assigned goal, and that can take actions such as sending communications, entering or modifying records, retrieving data from other systems, scheduling or triggering workflows with limited or no human review of each individual step. |
| **Autonomy Level** | The degree of human review required before, during or after an AI system takes an action, ranging from Suggest Only to Fully Autonomous (see Section 17.2). |
| **Scope of Authority** | A documented statement of what an agentic AI system may do, what it may not do, and what data and systems it may reach. |
| **Human Oversight** | The active role of qualified personnel in reviewing, validating and taking responsibility for any decision or action informed by AI. |
| **Publicly Accessible AI Tools** | AI platforms available to the general public via the internet without an institutional license or formal security review. User-provided data may be used to train AI models under the provider's own terms of service. |
| **Personal Paid Access to Publicly Accessible AI Tools** | AI tools purchased by employees using personal funds or personal accounts. These are treated as publicly accessible tools and are subject to all associated restrictions under this policy. |
| **Procured AI Tools** | AI platforms formally acquired or licensed by the Department through an approved procurement process and subject to required data security, privacy and contractual reviews. |
| **Sensitive Information** | Any data classified as confidential, protected or otherwise restricted under applicable law, regulation or Department policy. |
| **Material Change** | A change that could reasonably affect an AI system's intended use, functionality, outputs, risk classification, privacy or security protections, legal or regulatory compliance, accessibility, data sources, user population, or level of human oversight. |

Additional definitions relevant to the Department's operations (add as needed):

| Term | Definition |
|---|---|
| | |
| | |

# 7: Governance

The Department shall maintain an AI Governance Framework with defined oversight bodies and points of accountability. Governance responsibilities include policy enforcement, AI system review and approval, incident response, ongoing monitoring and compliance, and training and communication.

## 7.1. Governance Structure

The Department shall assign responsibility for the following AI governance functions:

- ☐ Overall policy authority and final decision-making
- ☐ Day-to-day AI policy coordination and issue triage
- ☐ Technical review
- ☐ Risk classification of AI tools
- ☐ Division or program-level implementation and compliance oversight
- ☐ Procurement documentation and AI tool inventory
- ☐ Workforce training documentation and disciplinary oversight
- ☐ Public communications related to AI use or incidents
- ☐ Assignment and review of autonomy levels for agentic AI systems
- ☐ Other _____

*Depending on the Department's size, structure, and governance approach, AI governance responsibilities may be assigned to individual staff members, an AI Governance Committee, or an existing committee with responsibility for AI oversight. In smaller departments, one or two individuals may fulfill multiple responsibilities, while larger departments may distribute them across multiple roles or committees. Regardless of the approach, each governance function described above should be clearly assigned to ensure accountability.*

## 7.2. Roles and Responsibilities

*Roles and Responsibilities Table*

| Role / Position | Core Responsibilities | Delegation of Authority |
|---|---|---|
| ***Example: Director / Health Officer (Replace with your role title and name)*** | *Provides overall authority, strategic direction and enforcement of the AI policy. Approves agency-wide AI policy, funding and resource allocation. Communicates expectations across divisions. Receives annual AI report. Makes final decisions on escalated issues.* | |
| **[Role Title — e.g., AI Point of Contact]** | | |
| **[Role Title — e.g., Information Technology (IT) / Technical Lead]** | | |

| Role / Position | Core Responsibilities | Delegation of Authority |
|---|---|---|
| [Role Title — e.g., Division / Program Manager] | | |
| [Role Title — e.g., Human Resources (HR) / Personnel Officer] | | |
| [Role Title — e.g., Data Privacy Officer] | | |
| All Staff (all appointment types, interns, volunteers) | | |
| Third Parties (contractors and vendors) | | |

## 7.3. Procurement and Consultant or Contractor Due Diligence

The Department must require consultants or contractors to (check all that apply):

- ☐ Meet all data-security, privacy, retention and deletion requirements before procurement is finalized
- ☐ Sign AI-related attestation and compliance forms
- ☐ Notify the Department of any incidents, breaches, failures or misuse involving their AI system
- ☐ Acknowledge the department's right to suspend or restrict access to any AI tool that pose a security, privacy, bias, operational or misuse risk
- ☐ Other: _____

## 7.4. Enforcement and Corrective Action

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

- ☐ Administrative or disciplinary action
- ☐ Suspension of data access privileges
- ☐ Termination of vendor contracts
- ☐ Referral to law enforcement (for willful violations)
- ☐ Other: _____

# 8: Overview of Acceptable Use and Prohibited Use

*Policy Principle: AI shall augment and not replace professional judgment, accountability and expertise.*

AI may be used when it (check all that apply):

- ☐ Advances the Department's mission and operational goals
- ☐ Has an assigned risk tier and required review appropriate to that tier
- ☐ Complies with all applicable Department policies and laws
- ☐ Operates under meaningful human oversight with safeguards proportional to risk
- ☐ Uses only approved Task–Tool pairings (see Section 10.6)
- ☐ Other: _____

Prohibited categories (see Section 13 for detailed rules and enforcement):

- ☐ High-risk functions performed in unapproved tools (e.g., processing protected health information (PHI) or personally identifiable information (PII), automating clinical or eligibility decisions, communicating unverified information to the public)
- ☐ Personnel misuse, including misinformation, unauthorized disclosure of confidential data, harassment/impersonation or bypassing security controls
- ☐ Agentic AI actions prohibited or restricted under Section 17 (e.g., actions taken at an unapproved autonomy level or outside a system's documented scope of authority)
- ☐ Other: _____

# 9: AI Notetaker: Approval and Disclosure Requirements

## 9.1. Overall Approach

The Department's rules for AI notetaking tools are (check all that apply):

- ☐ AI notetaking tools may be used only when approved by the meeting lead
- ☐ When a vendor, contractor or external party leads a meeting, approval authority for AI notetaking remains with the designated Department lead
- ☐ All meeting participants, internal and external, must be notified in advance when an AI notetaker is active
- ☐ The meeting lead must notify any participant who joins after the meeting has started that AI notetaking is active, before that participant's input is captured
- ☐ AI notetaking tools shall not be used to capture or process content prohibited under Section 9.5
- ☐ Notes or transcripts generated by AI (or manually, in lieu of AI) must be retained and disclosed consistent with the Department's public records obligations
- ☐ Other: _____

## 9.2. Internal Meetings With No External Participants

In addition to the overall approach outlined in 9.1, AI notetakers may be used in internal-only meetings when:

- ☐ The meeting lead has approved AI notetaking use; and
- ☐ No content prohibited under Section 9.5 is being discussed
- ☐ Other: _____

## 9.3. Meetings With External Partners

In addition to the overall approach outlined in 9.1, when collaborating with external partners, staff must (check all that apply):

- ☐ Confirm whether the partner permits the use of AI notetakers
- ☐ Ensure external participants may decline recording or AI transcription
- ☐ Confirm the AI notetaking vendor's data practices (e.g., whether recordings may be used for model training or accessed by third parties) before use with external partners
- ☐ Other: _____

## 9.4. Use of External AI Notetaking Tools Introduced by Partners

In addition to the overall approach outlined in 9.1, the following apply when an external partner brings their own AI notetaking tool to a meeting (check all that apply):

- ☐ External AI notetaking tools may only be used based on the Department's partner agreement
- ☐ Any request to use an external AI notetaking tool must be elevated to and approved by the meeting lead prior to the meeting
- ☐ External AI notetakers shall not be used when a meeting involves content prohibited under Section 9.5
- ☐ Staff have the right to decline the use of an external AI notetaking tool
- ☐ The Department has confirmed the external tool's data handling and retention practices, and that it will receive a copy of or access to any resulting transcript consistent with public records obligations
- ☐ Other: _____

When declining the use of an external AI notetaking tool, staff may use the following approved script:

> *"Thank you for your request to use an external AI note-taking tool. At this time, we are unable to authorize the use of external AI notetakers for this meeting. If there are no objections, we can enable an approved AI notetaking tool and will provide a meeting summary afterward. Thank you for your understanding."*

## 9.5. Prohibited Use of AI Notetaking Tools

AI notetakers may not be used in meetings where discussion includes (check all that apply):

- ☐ Confidential client or partner information
- ☐ Personally identifiable information (PII)
- ☐ Protected health information (PHI)
- ☐ Discussions involving legal counsel or legal consultation
- ☐ Personnel matters, HR topics or internal investigations
- ☐ Proprietary, pre-decisional or restricted content unless explicitly authorized
- ☐ Other: _____

In mixed-content meetings, staff must pause the AI tool during sensitive portions or avoid use entirely.

### 9.6. Approved Tools and Access Controls

The Department requires (check all that apply):

- [ ] Only agency-approved platforms with required privacy, security and data safeguards may be used
- [ ] Personal accounts, unapproved tools or unsecured platform versions may not be used for any agency business
- [ ] AI-generated notes must be stored only in approved agency locations
- [ ] Other: _____

### 9.7. Human Oversight and Quality Review

- [ ] AI-generated notes are considered drafts and must be reviewed by a designated staff member before use
- [ ] Final meeting documentation must meet agency quality standards
- [ ] Other: _____

### 9.8. Accountability and Incident Reporting

- [ ] Any accidental capture of sensitive or confidential information must be reported immediately to the designated supervisor
- [ ] Improper or unapproved use of AI notetakers may result in suspension of access, required retraining or other corrective action
- [ ] Other: _____

## 10: Risk and Tool Security Framework

The Department uses a unified Risk-Tier and Security-Level Framework to govern the responsible and secure use of AI. This framework aligns Task Risk Tiers (what AI is used for) with Tool Security Levels (what kind of system is being used) and applies to all AI-involved activities.

### 10.1. Tier A — High-Impact / Sensitive Tasks

Tasks involving PHI, PII or other regulated or sensitive data, or tasks that could directly affect services, eligibility determinations, benefits, client records or other mission-critical functions. Errors or misuse may cause significant harm.

Examples of Tier A tasks at this Department (add your own):

- [ ] Eligibility determination or benefit authorization
- [ ] Clinical decision support or triage
- [ ] Predictive analytics influencing care, prioritization or referrals
- [ ] Other: _____

Minimum required controls:

- [ ] Data security review prior to procurement — assigned to: [Title]
- [ ] Encryption of data in transit and at rest — assigned to: [Title]
- [ ] Human-in-the-loop oversight for critical decisions — assigned to: [Title]
- [ ] Approval prior to deployment — assigned to: [Title]
- [ ] Incident response notification within 24 hours — assigned to: [Title]

## 10.2. Tier B — Operational / Moderate-Risk Tasks

Tasks that support core operations by assisting with workflows, communications, scheduling, reporting, translation or program planning. Outputs may shape decisions or public messaging. Humans remain responsible for reviewing results.

Examples of Tier B tasks at this Department (add your own):

- ☐ Public information drafts or outreach content
- ☐ Translation of public-facing materials
- ☐ Scheduling or workflow automation
- ☐ Internal dashboards using aggregated or de-identified data
- ☐ Other: _____

Minimum required controls:

- ☐ Staff and QA review of outputs — assigned to [Title]
- ☐ Role-based access controls — assigned to: [Title]
- ☐ Confirmation that vendor meets basic privacy and data-protection standards — assigned to: [Title]
- ☐ Incident response notification within 24 hours to program lead — assigned to: [Title]

## 10.3. Tier C — Low Risk / Informational Tasks

Tasks involving only public or non-sensitive information, used for brainstorming, learning, creativity or early concept development. Outputs are informal drafts not used for official decisions or public communication.

Examples of Tier C tasks at this Department (add your own):

- ☐ Internal brainstorming, outlines or talking points
- ☐ Summaries of publicly available documents
- ☐ Grammar or readability suggestions on non-sensitive drafts
- ☐ Other: _____

Minimum required controls:

- ☐ Staff completes acceptable-use training; no PHI/PII/confidential input; treat outputs as drafts
- ☐ Supervisors guide on acceptable use and escalate repeated violations

## 10.4. Reclassification Rule

*If the scope, data sensitivity or level of automation of an AI task increases, reclassify to the higher tier and apply the corresponding controls immediately.*

## 10.5. Tool/System Security Levels (1 / 2 / 3)

Every AI tool and system must be assigned a security level aligned to data sensitivity and required safeguards.

| Security Level | Description | Minimum Controls |
|---|---|---|
| **Level 1 — High Security** | Systems and tools or uses that process, generate, analyze or store PHI, PII, confidential program records, regulated information or other sensitive data. Includes tools that could directly influence eligibility, benefits, workforce records, client records or other mission-critical decisions. | Encryption in transit and at rest; access controls with MFA; demonstrated security compliance (e.g., Service Organization Control 2 (SOC 2), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI RMF), Federal Risk and Authorization Management Program (FedRAMP)); data-residency controls; documented use case and decision boundaries; human approval for all outputs; 24-hour vendor and internal incident notification. |
| **Level 2 — Medium Security** | Systems and tools and systems that support core operations such as workflow, scheduling, communications, reporting, translation or data visualization. Errors are more likely to cause operational delays or confusion rather than direct harm. | No PHI/PII or confidential program data; vendor privacy and security practices confirmed; "No-train" or equivalent data-protection option enabled when available; appropriate access controls and logging; staff quality review before outputs are used; 24-hour incident notification. |
| **Level 3 — Low Security** | Systems and tools that only involve public, non-sensitive information and that are used for internal brainstorming, learning, creativity or early-stage concept development. Outputs are informal drafts not used for official decisions or public release unless reviewed. | No PHI/PII or confidential program data; "No-train" option enabled when available; basic user training on responsible use; 24-hour internal reporting if PHI/PII is accidentally entered or exposed. |

## 10.6. Task–Tool Combination Matrix

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

*Note: This matrix governs risk tier and tool security level only. Any AI system operating above Suggest Only autonomy (see Section 17.2) is also subject to the requirements of Section 17, regardless of its result in this matrix.*

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

## 10.7. Public and Personal Tool Use Rules

- [ ] Public and personal tools may only be used for Tier C tasks
- [ ] No PHI, PII, regulated, sensitive, internal or confidential data may be entered into public or personal tools
- [ ] Disable data-for-training and third-party sharing features where available
- [ ] Do not use AI tools that do not allow data-for-training and third-party sharing features to be disabled.
- [ ] If sensitive data may have been entered accidentally, notify the supervisor as soon as possible
- [ ] Other: _____

## 10.8. Intake, Cataloging and Reclassification

The Department must (check all that apply):

- [ ] Require all AI tools to obtain an initial risk classification prior to use
- [ ] Record all classifications in the AI Use Register / Approved Tools Catalog maintained by [designated role / office]
- [ ] Require a new classification review when scope of use, data sensitivity or level of automation increases
- [ ] Require reassessment and renewed authorization when there is a material change to the vendor, platform, or model used for high-risk tasks that could affect the tool's functionality, performance, risk profile, privacy, security, or compliance considerations.
- [ ] Update the Catalog at least quarterly, or when tools are approved or retired
- [ ] Other: _____

*All approved tools must be recorded in the AI Use Register / Approved Tools Catalog. See Appendix A and B for the complete tool inventory form.*

## 10.9. Acceptable Tool Use

The Department authorizes the following tool types (check all that apply):

- [ ] Procured Tools — may support Tiers A/B/C if security and oversight controls are met; must appear in the Approved Tools Catalog
- [ ] Public Tools — Tier C only; prohibited from PHI/PII/confidential data
- [ ] Personally Purchased Tools — treated as public tools; Tier C only; Tier A/B use is prohibited unless formally procured
- [ ] Other: _____

## 10.10. Oversight and Enforcement

- [ ] The designated technical reviewer oversees tool classification
- [ ] Division and program leads ensure tasks are correctly classified before use
- [ ] Repeated or intentional violations may result in tool suspension, access revocation and disciplinary action
- [ ] Other: _____

# 11: Human Competence and Acceptable AI Use

The Department establishes the following expectations to ensure that AI supports rather than substitutes for human skill development:

## 11.1. Staff Competencies and Readiness

Staff engaged in AI-supported work must (check all that apply):

- ☐ Possess, or be developing, the core competencies relevant to the tasks they perform
- ☐ Understand underlying processes well enough to evaluate AI outputs and identify errors or bias
- ☐ Gain foundational understanding of the relevant task before relying on AI
- ☐ Demonstrate the ability to complete or explain the task using conventional methods
- ☐ Other: _____

## 11.2. Integration Into Planning and Operations

- ☐ Staff shall document the intended role of AI during planning and implementation to ensure its use is appropriate and aligned with departmental goals
- ☐ The Department will not require formal skills assessments as a condition for AI use
- ☐ Other: _____

## 11.3. High-Risk or Complex Tasks

- ☐ AI systems should be used for high-risk or complex tasks only by staff with the expertise to perform the work independently or with a qualified colleague
- ☐ For lower-risk or routine tasks, AI may be used to support efficiency, learning and skill development
- ☐ Staff must continue to apply critical judgment and follow oversight procedures
- ☐ Other: _____

## 11.4. Situations Requiring Caution

Staff should pause or seek additional guidance before using AI when:

- ☐ They have not yet learned or practiced the core method or work function that AI supports
- ☐ Doing so would replace an essential learning opportunity, particularly for early-career staff
- ☐ Other: _____

# 12: AI Training and Readiness Requirements

Prior to using AI tools, systems or services for work, all applicable personnel shall complete required training. Completion of training is a condition of authorization to use AI.

## 12.1. Required Training Components

At minimum, required training shall cover (check all that apply):

- ☐ Introductory AI training covering capabilities, risks and responsible practices
- ☐ Ethical use, data privacy and security training consistent with Department standards and applicable laws
- ☐ Task-specific guidance for specialized or high-risk AI applications
- ☐ Rural AI literacy, including how AI-influenced decisions (e.g., risk scoring, outreach targeting, case prioritization, eligibility determination) may interact differently with rural access barriers such as distance to services, transportation and broadband limitations, and whether recommended next steps (e.g., referral, follow-up, service linkage) are available locally
- ☐ Training will be offered in formats accessible to staff with limited broadband access or travel capacity, such as asynchronous online modules, downloadable materials or regional in-person sessions
- ☐ Other: _____

## 12.2. Acknowledgment of Training

Upon completion of required training, staff must acknowledge (check preferred method):

- ☐ Signed written record of training completion and understanding
- ☐ Electronic attestation or completion form
- ☐ Learning Management System record
- ☐ Other: _____

All training acknowledgments shall be submitted to _____ for official recordkeeping.

## 12.3. Use Based on Risk Level

- ☐ Tier C (Low Risk) and Tier B (Moderate Risk): Staff may proceed with AI tool use after completing and acknowledging required foundational training
- ☐ Tier A (High Risk): Staff must complete training AND obtain approval from [Title] _____ prior to initiating any AI-supported activity

## 12.4. Documentation and Access Control

- ☐ Training completion and acknowledgment shall be documented and maintained by

  _____
- ☐ Access to AI tools may be limited or tiered based on whether acknowledgment and required approvals are on file
- ☐ Supervisors are responsible for ensuring compliance within their units
- ☐ Other: _____

### 12.5. Refresher Training

The Department may require refresher training when (check all that apply):

- ☐ Material changes to technology occur (e.g., major system updates or new AI platforms)
- ☐ Policies, legal standards or regulatory requirements related to AI, data privacy or information security are revised
- ☐ New organizational procedures affecting AI use are implemented
- ☐ Audit findings, incidents or compliance reviews indicate the need for additional training

*Training completion records and acknowledgments are maintained in Appendix E — Staff AI Training Completion Record.*

## 13: Prohibited and Misuse of AI

The Department prohibits the following AI functions and personal conduct to safeguard privacy, security, legal compliance and public trust.

### 13.1. Prohibited AI Functions (System-Level)

Unless expressly authorized under high-risk (Tier A), AI shall not be used for (check all that apply):

- ☐ Using unapproved systems to collect, process or store identifiable health or client information
- ☐ Making service or benefits decisions without required human review
- ☐ Issuing diagnoses, treatment recommendations or triggering interventions without qualified personnel oversight
- ☐ Publishing AI-generated content without communications or program review
- ☐ Using AI to make hiring, promotion or termination decisions without qualified personnel oversight
- ☐ Using proprietary or restricted data without explicit written authorization
- ☐ Entering client program records, subsidy or eligibility information into public or non-approved AI tools
- ☐ Uploading internal staff rosters, schedules, workforce lists or operational records into public or non-approved AI tools
- ☐ Inputting internal program documents into public or non-approved AI tools without authorization
- ☐ Using AI to analyze or summarize confidential operational data without proper authorization or risk classification
- ☐ Other: _____

*Agentic AI systems are additionally subject to the prohibited functions listed in Section 17.4*

### 13.2. Prohibited Personnel Conduct (Misuse)

The following conduct by staff, contractors, vendors, interns or volunteers is prohibited:

### *13.2.1. Misinformation, Deepfakes and Misrepresentation*

**Deepfake:** Synthetic or manipulated media created using artificial intelligence that realistically depicts a person, voice, image, or event and may falsely represent reality.

- ☐ Creating, disseminating or amplifying false, misleading or deceptive content using AI, including deepfakes or manipulated media
- ☐ Impersonating Department officials or misrepresenting Department activities through AI-generated content
- ☐ Other: _____

### *13.2.2. Unauthorized Use of Confidential or Sensitive Information*

- ☐ Inputting, uploading or disclosing PHI, PII, confidential data or other protected information into unapproved AI systems
- ☐ Other: _____

### *13.2.3. Personal Use Conflicting with Official Duties*

- ☐ Using Department resources, systems or credentials for personal projects or non-official activities
- ☐ Personal AI use that creates the appearance of Department endorsement or interferes with official duties
- ☐ Other: _____

### *13.2.4. Circumventing Security or Procurement Controls*

- ☐ Bypassing procurement, authorization or cybersecurity protocols by using unapproved AI tools for Tier A tasks
- ☐ Using personal accounts, unauthorized extensions or VPNs to access external AI platforms in violation of this policy
- ☐ Other: _____

### *13.2.5. Harassment and Discrimination*

- ☐ Using AI systems to harass, intimidate, impersonate or discriminate against any individual
- ☐ Generating offensive, threatening or discriminatory content or circulating such content
- ☐ Other: _____

### *13.2.6. Reporting and Enforcement*

Violations of this policy may result in (check all that apply):

- ☐ Verbal warning and additional training
- ☐ Written reprimand
- ☐ Suspension of AI access privileges
- ☐ Termination of employment or contract
- ☐ Referral to law enforcement (for willful violations)
- ☐ Other: _____

All personnel shall immediately report suspected or confirmed AI misuse to [Title] _____. Individuals who report violations in good faith will not face disciplinary action.

# 14: Contractor and Third-Party Obligations

## 14.1. Applicability and Compliance

All third-party entities performing work on behalf of the Department must (check all that apply):

- ☐ Comply with the principles, requirements and safeguards outlined in this policy
- ☐ Comply with applicable government-wide AI use policies and software acquisition requirements
- ☐ Ensure AI-enabled systems meet established standards for security, transparency and ethical operation
- ☐ Other: _____

## 14.2. Disclosure Requirements

### *14.2.1. Contractors and Consultants*

When entering into contractual agreements, contractors and consultants must:

- ☐ Disclose whether they intend to use AI technologies in the performance of any work or deliverables
- ☐ Provide a description of how AI will be applied, including tasks or deliverables it will support
- ☐ Explain how data privacy, security, bias, compliance and risk mitigation will be addressed
- ☐ Disclose whether the AI includes agentic capabilities, and if so, what actions it can take and what systems it can reach
- Other: _____

All contractor and vendor AI disclosures must be recorded at time of contract initiation. See Appendix C — Contractor and Vendor AI Disclosure Log.

### *14.2.2. Vendors*

When procuring or using AI-enabled products or services, departments should, where applicable and available:

- ☐ Review vendor documentation regarding AI-enabled features or functionality
- ☐ Review applicable terms related to data privacy, security, retention, sharing and breach notification
- ☐ Consult IT, procurement, privacy, security or legal staff when vendor AI practices or terms raise concerns
- ☐ Review vendor disclosures of agentic capabilities and configurable autonomy limits, consistent with Section 17.10
- ☐ Other: _____

## 14.3. Required Contract Language

Contractors and vendors must include the following AI Use Notification in contractual agreements when AI will be used in any part of the work:

> ***"The [Contractor/Consultant] acknowledges that [Department Name] has adopted organizational policies governing the responsible and ethical use of artificial intelligence (AI). The [Contractor/Consultant] agrees that any use of AI tools, models, platforms or services in connection with the performance of work under this agreement shall comply with those policies and all applicable laws and regulations."***

## 14.4. Review and Approval

- [ ] Contractors and consultants shall not implement or deploy any AI technology without prior written approval from the Department
- [ ] The Department reserves the right to review and reject any proposed AI use that poses unacceptable risks or fails to meet organizational standards

## 14.5. Ongoing Obligations

- [ ] Contractors and consultants shall promptly notify the Department of any material changes to their AI use during the term of the agreement
- [ ] Contractors and consultants shall cooperate with the Department in monitoring compliance with this policy
- [ ] Failure to comply may be considered a material breach of the agreement
- [ ] Other: _____

## 14.6. Applicability to Existing Contracts and Transition Period

This policy applies prospectively. For contractors and consultants with active contracts at adoption:

Standard transition period: _____ months from the effective date of this policy.

Extended transition period (for complex systems, by request): up to _____ months, subject to approval by _____.

- [ ] All contractors and consultants must disclose any current AI use during the transition period
- [ ] All new contracts initiated after the effective date must comply immediately
- [ ] All existing contracts must comply within the established transition period or upon renewal, amendment or extension
- [ ] Failure to meet transition requirements may affect eligibility for contract renewal or future procurements
- [ ] Other: _____

# 15: Responsible Use and Safeguards

## 15.1. Human Oversight

**Definition:** Human oversight means the active and informed involvement of designated personnel in reviewing, validating and taking responsibility for AI-generated outputs. Human oversight ensures that AI supports, rather than replaces, professional judgment and that final decisions remain under human authority. It includes monitoring for accuracy, fairness and alignment with ethical, legal and organizational standards.

For agentic AI systems, human oversight extends to reviewing and approving actions before, during or after they occur, consistent with the autonomy levels defined in Section 17.2, instead of only reviewing outputs after the fact.

The Department requires (check all that apply):

- ☐ All AI systems to operate under meaningful human oversight; AI outputs shall inform but not replace human judgment
- ☐ Personnel to review and validate AI-assisted outcomes for accuracy, fairness and compliance
- ☐ Level of human oversight to be proportionate to the risk classification of the AI application
- ☐ High-risk AI applications to require documented review and approval prior to deployment or use
- ☐ Personnel to refrain from relying on AI-generated outputs that appear inaccurate, incomplete or inconsistent with professional judgment
- ☐ All escalated cases to be logged in a centralized record or incident tracking system
- ☐ Significant or recurring AI-related issues to be reviewed for potential operational, privacy, security or vendor-related risks
- ☐ Personnel engaged in AI oversight to complete required training
- ☐ Escalation and incident response procedures will be established for high-risk AI concerns
- ☐ Agentic AI systems to operate at an autonomy level consistent with Section 17.3, with oversight and review appropriate to that level

When AI-generated results appear inaccurate or inconsistent with professional judgment:

- ☐ Low and Moderate Risk: Staff may rerun, recheck or adjust prompts to correct errors
- ☐ High Risk: Staff shall stop use of the output and escalate concerns to [Title] _____ for review, documentation and risk assessment

*All AI-related incidents, near-misses and escalated concerns must be documented. See Appendix D — AI Incident and Escalation Log.*

*Near-Miss is an AI-related incident that had the potential to cause harm, error, bias, privacy breach, or other negative consequences but was detected and addressed before affecting clients, staff, operations, or organizational decision-making.*

## 15.2. Bias Mitigation

**Definition:** Bias mitigation means taking specific steps to identify, reduce or prevent unfair patterns in how an AI system functions or produces results.

The Department requires (check all that apply):

- ☐ Proactive identification and mitigation of potential bias or inequitable outcomes in AI-assisted activities
- ☐ Vendors to disclose known limitations, performance concerns or populations for which the system may perform less reliably
- ☐ Vendors to provide information on how bias is addressed in training data, algorithms and expected outputs prior to procurement, as available
- ☐ Periodic review of AI outcomes for unintended bias, disparate impacts or inaccuracies, with findings shared with appropriate leads

- [ ] Staff training to include guidance on recognizing and addressing potential bias
- [ ] Documented processes for reporting, escalating and responding to identified bias, inequitable outcomes or AI-related concerns
- [ ] Corrective actions and mitigation measures to be documented and tracked
- [ ] Additional human review for AI-assisted activities involving historically underserved, disproportionately impacted or high-risk populations
- [ ] Additional human review for AI-assisted activities involving rural, frontier or geographically isolated populations, recognizing that AI systems trained primarily on urban-population data may perform less reliably for these communities
- [ ] 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, frontier and small-jurisdiction populations

## 15.3. Transparency

**Definition:** Transparency means providing clear, accessible and accurate information about how AI systems are used, what they do and how they influence decisions. It applies to both internal (e.g., staff, leadership, partners) and external (e.g., community members, partner organizations, other agencies) stakeholders.

The Department shall maintain openness about its use of AI in operations, communications and decision-making.

The Department's transparency approach includes (check all that apply):

- [ ] Maintaining an AI Use Register accessible to staff
- [ ] Publishing a public-facing summary of how the Department uses AI
- [ ] Notifying community members when AI is used in decisions that affect their services or benefits
- [ ] Issuing public communications when significant AI incidents occur
- [ ] Providing transparency information through channels accessible without reliable broadband (e.g., printed notices, in-person communication) for rural and underserved communities
- [ ] Other: _____

## Documentation requirements by risk level:

### *High-Risk Use (Tier A):*

- [ ] Detailed documentation is required in the AI Use Register for all Tier A AI use, including purpose, role, data sources, safeguards and decision logic

Complete the following for each Tier A AI use:

AI tool or system used: _____

Purpose of AI use: _____

Data sources involved: _____

Safeguards in place: _____

How final decisions are made (human role):

_____

Sample documentation statement (adapt as needed):

> *"AI was used to support [describe task] by [describe AI's role]. Final decisions were made exclusively by [role title] at [Department Name]."*

### *Moderate-Risk Use (Tier B):*

- [ ] A disclaimer is required on all documents or communications produced with AI assistance
- [ ] The designated lead shall determine on a case-by-case basis whether a disclaimer is required
- [ ] Other: _____

Sample disclaimer (adapt as needed):

> *"AI was used to [describe task; e.g., compare findings and generate an initial draft]. The content was reviewed and edited by [Department Name] staff for accuracy and alignment with departmental standards."*

### *Low-Risk Use (Tier C):*

- [ ] No formal disclosure is required for Tier C use; responsible use practices still apply
- [ ] Other: _____

## 15.4. Data Privacy

**Definition:** Data privacy refers to the protection of personal, sensitive and confidential information from unauthorized access, use, disclosure, alteration or destruction. Data privacy ensures individuals maintain control over their data and that all handling of such information aligns with legal, ethical and organizational standards.

The Department requires (check all that apply):

- [ ] All AI-related activities to comply with applicable privacy, confidentiality and data protection laws, regulations and Department policies
- [ ] Only the minimum amount of data necessary to be collected, used, stored or disclosed
- [ ] Individuals to be informed when their data is used in AI-supported processes; where required, informed consent must be obtained
- [ ] All contractors, consultants should comply with Department privacy requirements
- [ ] No AI system to be trained or improved using Department data without prior written authorization
- [ ] Data to be retained and disposed of in accordance with Department records management standards
- [ ] Other: _____

## 15.5. Data Security

**Definition:** Data Security refers to administrative, technical and physical safeguards designed to protect data from unauthorized access, use, disclosure, alteration or destruction.

The Department requires (check all that apply):

- [ ] All AI tools and systems to follow security safeguards associated with their assigned Security Level
- [ ] Sensitive, confidential or regulated data to be encrypted in transit and at rest when processed through Level 1 or Level 2 AI systems
- [ ] Access to AI systems to follow appropriate access controls based on the designated security level
- [ ] Only Department-approved AI tools and systems to be used for any activity involving Department data
- [ ] Vendors to meet minimum-security expectations for their security level, including 24-hour incident notification
- [ ] "No-train" or equivalent data-protection features to be enabled when available
- [ ] Users to report any suspected exposure of sensitive data or unauthorized access within 24 hours
- [ ] Other: _____

# 16: Acquisition of AI Tools and Systems

## 16.1. Authorization and Review

Before acquiring or subscribing to any AI tool or service, staff must submit a written request to [Title] _____ that describes the tool's purpose, functionality, data use, risk classification and anticipated impact and assigned autonomy level for any agentic capabilities (see Section 17.2).

For Tier B (moderate-risk) tools, the following reviews are required (check all that apply):

- ☐ Technical review, including security, data handling and integration
- ☐ Policy and governance review, including risk classification and minimum controls
- ☐ Notification to appropriate tracking and documentation leads
- ☐ Other: _____

For Tier A (high-risk) tools, the following reviews are required (check all that apply):

- ☐ Full review and approval by the technical reviewer, governance lead and oversight office
- ☐ Division-level approval alone is not sufficient for Tier A systems
- ☐ Other: _____

## 16.2. Risk-Based Classification of AI Tools

- ☐ All procured AI systems shall undergo a risk-based classification process prior to procurement, deployment or use
- ☐ Each tool shall be assessed by the designated governance body in coordination with the technical reviewer and division leads
- ☐ The AI Use Register shall include the responsible division, program purpose and assigned risk tier for each tool
- ☐ Other: _____

## 16.3. Oversight and Reclassification

- ☐ The designated lead shall maintain a record of all AI tools in use, their assigned security tier and corresponding reporting requirements
- ☐ The governance body shall conduct periodic reviews to ensure tools remain properly classified
- ☐ Any tool whose use expands to include sensitive data or functions shall be reclassified and brought into compliance with higher-tier requirements
- ☐ Other: _____

## 16.4. Procurement Standards

All AI acquisition contracts shall include clauses requiring (check all that apply):

- ☐ Disclosure of any AI components or automated decision-making functions
- ☐ Compliance with Department data privacy and security policies
- ☐ Vendor cooperation in audits and compliance reviews
- ☐ Prohibition on secondary use of Department data without written authorization
- ☐ Notification of any material changes to the AI system that may affect risk, data handling or functionality
- ☐ Vendor disclosure of how the tool performs in rural, small-jurisdiction or low-connectivity settings, including known limitations and plain-language documentation of conditions under which performance may vary
- ☐ Disclosure of any agentic or autonomous action capabilities and the Department's ability to configure, restrict or disable them
- ☐ Other: _____

Preference shall be given to AI tools that provide (check all that apply):

- ☐ Explainability features
- ☐ Compliance with ADA standards
- ☐ Human-in-the-loop capabilities
- ☐ Data minimization practices
- ☐ Documentation of model performance
- ☐ Vendor participation in regional, multi-county or state-level procurement consortia, to improve access and terms for Departments with limited independent purchasing power
- ☐ Other: _____

## 16.5. Recordkeeping and Inventory Management

- ☐ The Department shall maintain a centralized register of all approved and active AI systems, documenting system name, purpose, vendor, approval date, risk classification and responsible division
- ☐ Divisions must report any changes to system use, purpose or configuration to [Title] _____ within ____ days.
- ☐ Each authorized AI tool shall undergo review by the designated lead at least annually
- ☐ Other: _____

## 16.6. Decommissioning and Termination

- ☐ An AI system shall be decommissioned when no longer required, when it has reached end of service life or when it fails to meet compliance standards
- ☐ Prior to decommissioning, all associated data shall be reviewed for archival, transfer or destruction in accordance with Department records management and privacy policies
- ☐ Other:

## 16.7. Continuous Improvement

- ☐ Designated governance leads shall monitor emerging AI technologies and assess their potential applicability to Department operations
- ☐ Divisions shall document lessons learned following pilot programs or system retirements
- ☐ Findings from acquisition reviews shall inform updates to this policy and related procedures

# 17: Agentic AI Systems

Agentic AI systems differ from other AI tools in that they take actions rather than only produce outputs for a person to review. Because the point of human review shifts from "before the output is used" to "before, during or after the action is taken," these systems require controls beyond those in Sections 10 and 15.

**Definition: Agentic AI.** An AI system that plans and carries out multi-step tasks toward an assigned goal, and that can take actions — such as sending communications, entering or modifying records, retrieving data from other systems, scheduling or triggering workflows with limited or no human review of each individual step.

## 17.1. Scope

This section applies whenever an AI system (check all that apply):

- ☐ Takes actions in a system of record, program database or shared file location
- ☐ Sends, schedules or posts communications to staff, partners or the public
- ☐ Retrieves or combines data from multiple sources without step-by-step direction
- ☐ Operates on a schedule, trigger or standing instruction rather than a single request
- ☐ Uses credentials, accounts, integrations or connectors to reach other systems
- ☐ Other _____

*Agentic features added to a previously approved tool constitute a material change under Section 10.8 and require reassessment and renewed authorization before the feature is enabled or used.*

## 17.2. Autonomy Levels

Every authorized agentic use shall be assigned one of the following autonomy levels, documented in the AI Use Register:

| Autonomy Level | Description |
|---|---|
| **Suggest Only** | The system proposes actions; a staff member performs each action. |
| **Act With Approval** | The system prepares actions and executes them only after documented staff approval of each action. |
| **Act and Report** | The system executes defined actions within pre-set limits and reports them to a named reviewer within a defined period. |
| **Fully Autonomous** | The system executes actions without individual approval or routine review. |

## 17.3. Permitted Autonomy by Risk Tier

| Task Tier | Suggest Only | Act With Approval | Act and Report | Fully Autonomous |
|---|---|---|---|---|
| **Tier A — High Risk** | **Allowed** | **Allowed, subject to full governance review under Section 17.5** | **Prohibited** | Prohibited |
| **Tier B — Medium Risk** | **Allowed** | **Allowed** | **Allowed with logging and a named reviewer** | Prohibited |
| **Tier C — Low Risk** | **Allowed** | **Allowed** | **Allowed** | Allowed only for internal, non-sensitive tasks with no external action |

***Hard Guardrail:*** *No agentic system may take an action that is irreversible, externally visible or that affects an individual's services, benefits, eligibility or care without documented human approval before the action occurs.*

## 17.4. Prohibited Agentic Functions

Regardless of tier or approval, agentic systems shall not (check all that apply):

- ☐ Determine, deny, modify or terminate eligibility, benefits or services
- ☐ Initiate clinical, case management or investigative actions affecting an individual
- ☐ Send public-facing communications, media statements or emergency messaging without review
- ☐ Communicate directly with clients, patients or community members without disclosure that AI is in use and without a documented staff reviewer
- ☐ Enter, alter or delete records in a system of record without an approved, reversible and logged process
- ☐ Obligate funds, submit reports to state or federal partners, or file regulatory submissions
- ☐ Grant, modify or revoke system access or user permissions
- ☐ Create, deploy or authorize other agents or automated processes
- ☐ Other: _____

## 17.5. Authorization Before Deployment

Requirements in Sections 17.5-17.9 apply in full to Tier A and Tier B agentic uses. For Tier C agentic uses, the Department may apply a streamlined version of these requirements, at the discretion of [Title] _____, in proportion to the limited risk involved.

Before any agentic use is enabled, the Department requires (check all that apply):

- ☐ A written scope of authority stating what the agent may do, what it may not do, and what data and systems it may reach
- ☐ Assigned risk tier, tool security level and autonomy level, recorded in the AI Use Register
- ☐ A named accountable staff member for each authorized agent — accountability may not be assigned to a team in the abstract
- ☐ Approval consistent with Section 16.1 for the assigned tier; Tier A agentic use requires full governance review
- ☐ A defined test or limited pilot period before full deployment
- ☐ Documented rollback procedure for actions the agent can take
- ☐ Other: _____

## 17.6. Human Oversight and Stop Conditions

The Department requires (check all that apply):

- ☐ A staff member with authority to pause, restrict or terminate an agent's operation at any time, without vendor involvement
- ☐ Defined conditions under which the agent must stop and escalate rather than proceed, including uncertainty, missing data, conflicting instructions or an action outside its scope of authority
- ☐ Review of agent activity by the accountable staff member at a defined interval appropriate to tier
- ☐ Escalation to [Title] _____ when an agent acts outside its authorized scope
- ☐ Staff authority to reverse or disregard any agent action without justification to the vendor or the system
- ☐ Other: _____

## 17.7. Agent Identity, Access and Credentials

The Department requires (check all that apply):

- ☐ Agents to operate under a distinct, identifiable account rather than a staff member's personal credentials
- ☐ Access limited to the minimum systems and data needed for the authorized scope
- ☐ Time-limited or renewable access, reviewed at least annually
- ☐ Immediate revocation of agent access when the authorized use ends, the accountable staff member changes or the tool is decommissioned
- ☐ Agent-generated communications to be identifiable as such to recipients
- ☐ Other: _____

## 17.8. Logging, Records and Auditability

The Department requires (check all that apply):

- ☐ A retained log of agent actions sufficient to reconstruct what was done, when, on whose authority and on what data
- ☐ Logs retained in accordance with Department records management standards and applicable open records law
- ☐ Agent actions taken on Department business to be treated as Department records
- ☐ Logs to be reviewable by staff without vendor assistance
- ☐ Agent activity included in periodic bias and outcome review under Section 15.2
- ☐ Other: _____

*Agent-related errors, out-of-scope actions and near-misses are documented in Appendix D — AI Incident and Escalation Log.*

## 17.9. Untrusted Content and Instruction Integrity

Agentic systems can encounter instructions embedded in the content they process — in email, uploaded files, web pages or partner submissions — and may act on them. The Department requires (check all that apply):

- ☐ Agents that process externally supplied content to be restricted from taking consequential actions based on that content without human review
- ☐ Staff training on this risk for anyone operating or supervising an agent
- ☐ Vendor disclosure of what safeguards exist against instructions embedded in processed content
- ☐ Reporting of any suspected instance to [Title] _____ as an AI incident
- ☐ Other: _____

## 17.10. Vendor and Procurement Requirements

In addition to Sections 14 and 16.4, contracts for agentic AI shall require (check all that apply):

- ☐ Disclosure of all actions the system is capable of taking and all systems it can reach
- ☐ Disclosure of any subprocessors, models or external services the agent calls during operation
- ☐ Notification before agentic capabilities are added to, expanded within or enabled by default in a procured tool
- ☐ Department ability to configure autonomy limits, disable specific actions and disable the agent entirely
- ☐ Department access to complete action logs in an exportable format
- ☐ Documentation of how the system behaves on failure, timeout or loss of connectivity
- ☐ Other: _____

## 17.11. Monitoring, Reclassification and Decommissioning

The Department requires (check all that apply):

- [ ] Review of each authorized agent at least annually, and whenever its scope, data access or autonomy level changes
- [ ] Reclassification to a higher tier or lower autonomy level when scope, data sensitivity or potential impact increases
- [ ] Decommissioning of agents no longer in active use, including revocation of all associated access
- [ ] Review of retained data, logs and integrations prior to decommissioning, consistent with Section 16.6
- [ ] Other: _____

## 17.12. Training

Staff who operate or supervise agentic systems shall complete training covering (check all that apply):
The assigned scope of authority and how to recognize action outside it

- [ ] How to pause, stop and reverse agent actions
- [ ] Reviewing a log of actions rather than a single output
- [ ] Instruction-integrity risk in externally supplied content
- [ ] Escalation and incident reporting requirements under Section 15.1
- [ ] Other: _____

# 18: Review, Revision and Effective Date

## 18.1. Policy Review Cycle

This policy shall be reviewed at least (check one):

- ☐ Annually
- ☐ Every two years
- ☐ Other: _____

The policy shall also be reviewed when required by legislative, regulatory or organizational changes.

## 18.2. Responsible Entity

**The policy review and revision process shall be coordinated by:** _____

## 18.3. Revision Process

- ☐ Proposed amendments may be initiated by any Department division or designated governance lead
- ☐ All proposed revisions shall undergo internal review
- ☐ Revisions must be approved by the designated governance body
- ☐ Once approved, the updated policy shall be communicated to all staff, contractors and partners and posted on designated platforms
- ☐ Other: _____

## 18.4. Interim Updates

In the event of urgent regulatory, legal or operational changes, the designated governance body may issue interim guidance prior to the next formal review cycle. Such updates shall be incorporated into the next full policy revision.

## 18.5. Effective Date

**This policy shall take effect on:** _____

## 18.6. Archiving of Previous Versions

All superseded versions of this policy shall be retained in accordance with Department records management protocols.

# Policy Acknowledgment and Approval

| | |
|---|---|
| **Approved by:** | |
| **Title:** | |
| **Date:** | |
| **Reviewed by:** | |
| **Title:** | |
| **Date:** | |

# Staff Acknowledgment

| | |
|---|---|
| **Signature:** | |
| **Printed Name:** | |
| **Title:** | |
| **Date:** | |

| Revision Number | Section / Pages Revised | Date | Description of Change |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# **Appendix A:** AI Use Register / Approved Tools Catalog

*Maintained by [designated role / office]. Update at least quarterly or when tools are added, approved or retired. The AI Use Register lists which tools are authorized and what they can be used for. Tools not in the Register may only be used for Tier C tasks.*

| Tool / System Name | Vendor / Provider | Risk Tier (A / B / C) | Security Level (1 / 2 / 3) | Rural Validation Status | Known Limitations Documented (Y/N) | Approval Date | Responsible Division | Status (Active / Retired) |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

*Note: Add rows as needed. All fields required before tool may be used.*

# **Appendix B:** Approved Tier A (High-Risk) AI Tools — Extended Documentation

*Tier A tools require full documentation per Section 15.3. Complete all fields before deployment. Division-level approval alone is not sufficient.*

| Tool / System Name | Vendor / Provider | Risk Tier (A / B / C) | Security Level (1 / 2 / 3) | Approval Date | Responsible Division |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# **Appendix C:** Contractor and Vendor AI Disclosure Log

*Record all contractor and vendor AI disclosures. Update when new contracts are initiated or when contractors notify the Department of changes to their AI use.*

| Contractor / Vendor Name | Contract Start Date | AI Use Disclosed? (Yes / No / N/A) | Compliance Status | Notes / AI Description |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# **Appendix D:** AI Incident and Escalation Log

*Document all AI-related incidents, near-misses, bias findings and escalated concerns. Required for Tier A tools; recommended for all tiers.*

| Date | Tool / System Involved | Incident Type (Error / Bias / Breach / Other) | Risk Tier Affected (A,B or C) | Incidence Severity (Low / Moderate / High) | Reported By (Title) | Status (Open / Resolved) | Description and Resolution |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

# **Appendix E:** Staff AI Training Completion Record

*Maintained by [designated role]. All staff must complete required training before using AI tools. Tier A users also require supervisor approval on file.*

| Staff Name / Title | Division | Training Completed (Date) | Acknowledgment Method | Tier A Approval (if applicable) | Supervisor Confirmation |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Notes

# Notes


PHIG
PARTNERS
SHAPING TOMORROW'S PUBLIC HEALTH TODAY.


KANSAS HEALTH INSTITUTE
Informing Policy. Improving Health.