UT Southwestern Medical Center

AI-Data Governance Policy Document
Aligned with the U System-Wide REAL Health AI Framework (Responsible, Ethical, Accountable, Legal)

---

1. Purpose and Scope

This policy outlines the governance, compliance, and ethical standards guiding the acquisition, management, processing, and deployment of Artificial Intelligence (AI) systems and health data at UT Southwestern Medical Center. It ensures alignment with:
- The UT System REAL Health AI Initiative
- Regulatory frameworks: HIPAA, PHI protections
- Clinical data standards: SNOMED CT, ICD-10
- Enterprise architecture and security guidelines

2. Guiding Principles (REAL Framework)

🟩 Responsible
- Ensure AI systems are clinically validated, auditable, and explainable
- Adopt model cards, drift monitoring, and bias detection
- Prioritize human-in-the-loop design for safety-critical workflows

🗨 Ethical
- Promote fairness, non-discrimination, and inclusivity
- Transparently communicate risks, limitations, and intended use of AI
- Enable consent-aware research and transparent opt-out policies

🟧 Accountable
- Assign accountability for each model's lifecycle: design, deployment, maintenance
- Use CI/CD pipelines with audit trails and approval checkpoints
- Establish clear data stewardship responsibilities across academic, clinical, and research units

🔴 Legal
- Ensure compliance with HIPAA, Texas privacy laws, FDA guidelines, and IRB protocols
- All handling of PHI must follow access controls, masking, and encryption standards
- Incorporate data use agreements (DUAs) and Business Associate Agreements (BAAs) into external collaborations

3. Data Architecture & Standards

3.1. Data Sources

AI solutions must draw from well-documented, curated datasets, including:
- EHR systems: Epic, Cerner
- Research repositories: Clinical Research Warehouse (~50TB+)
- Operational Data Stores (ERP)

3.2. Coding Standards

- SNOMED CT must be used for clinical concept standardization
- ICD-10-CM/PCS must be used for diagnosis and procedure classification
- AI training datasets must be validated against these standards

3.3. Synthetic Data Generation

- Azure-based synthetic data tools are authorized to enable model development in PHI-restricted settings
- All synthetic data must be statistically validated and privacy-enhanced

Section 4: Data Governance Infrastructure

Purpose: To define how data governance tools, architecture, and security controls will support safe, compliant, and reliable AI development.

4.1. Data Mesh Model

- Decentralized domain-driven ownership is supported to encourage innovation and agility.
- Governance remains centralized to ensure standardization of metadata, access protocols, and privacy safeguards.
- All data-producing domains are required to document their data products in a **Purview-based enterprise catalog**.
- Domains must define Data Product Owners responsible for stewardship and lineage tracking.

4.2. Unity Catalog Integration

- Unity Catalog is the system of record for all data access management, lineage, and classification.
- Data products must:
    - Be **registered with metadata**, including origin, version, and classification.
    - Be **access-controlled** through role-based policies aligned with zero-trust architecture.
    - Include **lineage visibility** from raw ingestion through AI model training and output generation.
- Developers and users must request access via formal workflows that log every interaction and permission change.

4.3. Cloud Governance

- All AI and data engineering workloads must run in UT Southwestern's **Azure environment**.
- **Azure Machine Learning (Azure ML)** and **Azure Synapse** will serve as the primary execution layers.
- Production environments must be provisioned using **Infrastructure-as-Code (IaC)** for consistency and auditability.

- Encryption at rest and in transit is enforced using approved enterprise key management systems.
- Continuous security monitoring, patching, and configuration compliance must be in place for all virtualized services.

Section 5: AI Lifecycle Governance

Purpose: To define governance controls for each phase in the AI solution development and deployment pipeline.

Phase	Governance Measures
Design	Bias assessment plan, stakeholder inclusion, compliance checklist
Data Collection	DUAs, SNOMED/ICD mapping, PHI masking/de-identification
Training	Model transparency reports, explainability (SHAP/LIME), synthetic data approval logs
Validation	Internal peer review, test coverage, clinical expert sign-off
Deployment	MLOps pipeline integration (CI/CD, rollback, audit logging)
Monitoring	Fairness dashboard, drift detection, privacy audit trail

Phase Descriptions and Controls:

- **Design**
  - Develop use-case aligned with institutional and ethical goals
  - Conduct stakeholder engagement sessions to define success metrics
  - Complete model bias risk assessments and compliance readiness checklists
- **Data Collection**
  - Ensure presence of executed DUAs or IRB protocols
  - Validate correct mapping to SNOMED CT and ICD codes
  - Enforce PHI de-identification protocols or synthetic data substitution
- **Training**
  - Maintain transparency documentation (e.g., Model Cards, version logs)
  - Use SHAP, LIME or equivalent techniques for model explainability
  - Store signed synthetic data approvals where applicable
- **Validation**
  - Require cross-disciplinary peer review (clinical + technical)
  - Ensure adequate performance benchmarks across populations
  - Capture approval from a designated clinical expert
- **Deployment**
  - Integrate model into CI/CD pipeline with rollback capabilities
  - Use Azure ML logging, monitoring, and version control tools
  - Secure environment settings with audit-logging and alerting
- **Monitoring**
  - Track model drift using statistical monitoring techniques
  - Maintain fairness dashboards and revalidation triggers
  - Log all runtime exceptions, escalations, and resolution notes

Section 6: Model Risk Categorization

Purpose: To stratify AI use cases based on risk exposure and apply commensurate governance controls for responsible development and deployment.

Risk Tier	Examples	Controls Required
Tier 1 (High)	Diagnostic AI, Clinical Decision Support	IRB Approval, Clinical Validation, Human Oversight, External Peer Review, Audit Trail
Tier 2 (Medium)	Operational ML (e.g., scheduling, forecasting)	QA Testing, Accuracy Benchmarking, Business Sponsor Sign-Off, Access Controls
Tier 3 (Low)	NLP summarization for internal communications	Internal Code Review, Logging, Limited Access, Periodic Monitoring

Tier 1 – High Risk

AI systems that influence or guide clinical decisions, patient diagnosis, or treatment pathways. These models require the most stringent controls, including:

- Institutional Review Board (IRB) approval
- Human-in-the-loop operationalization
- Clinical domain expert validation
- Frequent retraining and fairness audits
- Responsible AI documentation (model cards, error analysis, confidence scoring)

Tier 2 – Medium Risk

AI systems that support operational decisions (e.g., resource allocation, scheduling) or administrative functions that indirectly affect care quality.

- Business use-case alignment
- QA regression testing with error tracking
- Sponsor and stakeholder approval
- Monitoring for unintended workflow bias or drift

Tier 3 – Low Risk

AI solutions that offer assistive functions with no direct impact on patient outcomes (e.g., summarization of provider notes for internal documentation).

- Minimum viable governance
- Logging and change tracking
- Internal usage agreement (when applicable)

Risk tier classification must be declared in the Data Use Registry (Section 1), validated during Compliance Sign-Off (Section 3), and approved prior to any public dissemination (Section 2).

Section 7: Roles and Responsibilities

Purpose: To define role-specific responsibilities across the data and AI lifecycle to ensure accountability, continuity, and clear ownership.

Role	Responsibilities
Director of AI	Leads AI strategy, oversees innovation pipelines, aligns AI efforts with institutional goals and CDO vision. Responsible for REAL AI integration and Center of Excellence development.
Chief Data Officer (CDO)	Owns enterprise data strategy including cloud transition, mesh architecture, and governance policies. Ensures integration of AI initiatives with enterprise infrastructure.
Chief Health Information Officer (CHIO)	Ensures alignment of clinical AI applications with health informatics strategies. Provides clinical validation oversight and supports responsible deployment into care workflows.
Data Stewards	Manage metadata, data quality, schema harmonization, and access controls. Ensure compliance with Purview and Unity Catalog documentation requirements.
Data Governance Committee	Reviews and updates governance policies, oversees external data use requests, manages DUAs, and escalates ambiguous use cases. Maintains compliance with HIPAA and UT System standards.
AI Engineering Team	Builds and maintains pipelines for data ingestion, model training, CI/CD deployment, drift monitoring, rollback capabilities, and audit logging. Collaborates with data scientists, IT, and compliance.
Legal Counsel & IRB	Reviews all AI deployments involving PHI or public dissemination. Ensures compliance with HIPAA, federal and state laws, and institutional policies.
Clinical Champions	Act as domain experts during AI validation and implementation phases. Provide feedback, lead user testing, and advocate for clinical adoption.

Roles may overlap or evolve as the AI program matures. Each project should document role assignments as part of its Compliance Sign-Off (Section 3).

Section 8: Ethics and Review Process

Purpose: To ensure that all AI-related initiatives are thoroughly vetted for ethical soundness, legal compliance, clinical relevance, and operational feasibility.

All AI solutions must pass through a **Multidisciplinary Review Board (MRB)** prior to validation, deployment, or dissemination. The MRB must include representation from:

- **Informatics** – to assess data integrity, interoperability, and alignment with IT strategy
- **Ethics** – to evaluate fairness, bias, consent practices, and respect for persons
- **Legal/IRB** – to review compliance with HIPAA, PHI standards, DUAs, and IRB protocols
- **Clinical Stakeholders** – to verify clinical relevance, safety, and outcome utility

Each AI submission will be evaluated for:

- **Real-world impact** – tangible value to patient care, research, or operations

- **Bias risk** – presence of demographic, systemic, or algorithmic bias; proposed mitigation strategies
- **Data provenance** – clarity on dataset origin, coding standards (e.g., SNOMED, ICD), and data custodianship
- **Regulatory posture** – status of IRB/DUA compliance, model risk tier, and PHI handling safeguards

Review Outcomes May Include:

- Approved for pilot
- Approved with conditions
- Request for revision/resubmission
- Rejected due to risk, ethics, or technical limitations

All MRB decisions must be documented and submitted to the Data Governance Committee and included in the project's Compliance Sign-Off (Section 3). Periodic re-review may be triggered by material model changes, performance drift, or data source updates.

Section 9: Education and Awareness

Purpose: To build institutional capacity, ensure ethical literacy, and promote responsible AI adoption through continuous learning and stakeholder engagement.

9.1. Training Programs

- **Mandatory onboarding** sessions for new AI practitioners, researchers, and data stewards
- **Annual refreshers** on AI governance, HIPAA/PHI compliance, and emerging best practices
- **Department-specific workshops** tailored for clinical, operational, and research units

9.2. Curriculum Content

Training materials shall include:

- Principles of the **REAL AI Framework** (Responsible, Ethical, Accountable, Legal)
- Overview of AI Lifecycle Governance and Risk Tiers (Sections 5 & 6)
- Standards for SNOMED, ICD coding, and data harmonization
- Safe use of synthetic and de-identified data
- Fairness, bias detection, and model explainability
- IRB and DUA processes and obligations
- Responsible AI tools and documentation practices (e.g., model cards, transparency reports)

9.3. Stakeholder Engagement

- Organize quarterly **Town Halls** and **AI Roundtables** for feedback, knowledge sharing, and updates on institutional priorities

- Maintain a centralized **Knowledge Hub** or portal with updated templates, FAQs, workflows, and case studies
- Disseminate updates via **newsletters**, **email briefs**, or **intranet alerts** as policy or tool changes occur

9.4. Monitoring & Evaluation

- Track training participation through learning management systems (LMS)
- Evaluate comprehension via pre/post assessments or scenario-based evaluations
- Collect and act on feedback to improve content quality and relevance

Education is required for compliance and institutional alignment. Participation may be enforced as part of access provisioning or project sign-off milestones.

Section 10: Versioning and Change Management

Purpose: To ensure that the AI governance policy remains responsive to technological evolution, institutional needs, and regulatory updates through structured version control and stakeholder oversight.

10.1. Policy Version Control

- All versions of the AI-Data Governance Policy shall be **tracked with date, version number, and summary of changes**.
- Version updates must be **archived and accessible** via the institutional knowledge portal.
- Every version must include a footer indicating approval date and responsible committee.

10.2. Change Approval Process

- **Minor updates** (e.g., typographical corrections, link updates) may be approved by the Director of AI and logged.
- **Major updates** (e.g., role redefinitions, risk tier adjustments, data standard changes) require formal review and approval by the **Data Governance Committee and CDO**.
- **Emergency amendments** may be issued under joint authority of the CDO and Legal Counsel but must be retroactively reviewed within 30 days.

10.3. Stakeholder Notification

- All approved policy changes must be **communicated to relevant stakeholders** via institutional channels (e.g., email, LMS notification, leadership meetings).
- Affected project teams must acknowledge receipt of any policy revisions that impact their active use cases or workflows.

10.4. Audit & Review Frequency

- This policy shall be formally reviewed **at least semi-annually** by the Data Governance Committee.
- A review log should be maintained and made available to auditors upon request.

- Insights from audits, compliance incidents, or post-mortem reviews may trigger off-cycle updates.

The goal of this process is to balance agility in adapting to new AI paradigms with accountability, transparency, and institutional consensus.

Section 11: Enforcement

Purpose: To define the mechanisms and consequences for ensuring compliance with the AI-Data Governance Policy and protecting institutional integrity.

11.1. Compliance Monitoring

- Compliance with this policy will be tracked through:
    - Internal audits of AI model documentation, access logs, and DUA/IRB adherence
    - Periodic review of Data Use Registry and Compliance Sign-Off forms
    - Reports generated from Azure ML and Unity Catalog logs

11.2. Reporting Violations

- Any suspected violations of this policy must be reported to the **Data Governance Committee** and **Office of Compliance**.
- Reports may be submitted confidentially via designated compliance channels.
- The committee will initiate an investigation and involve Legal Counsel and IRB as needed.

11.3. Consequences of Non-Compliance

Violations of this policy may result in one or more of the following actions:

- **Revocation of access** to institutional datasets, platforms, or tools
- **Suspension or decommissioning** of the AI system in question
- **Corrective action plans**, including retraining or redevelopment under supervision
- **Institutional disciplinary measures** aligned with HR and legal policies
- **Termination** of data-sharing agreements or external collaborations

11.4. Escalation and Appeals

- Stakeholders may request reconsideration or appeal enforcement actions through a formal process managed by the Data Governance Committee.
- Appeals must be submitted within 30 days of the enforcement notice and include supporting documentation.

Maintaining a culture of responsible AI development and use requires proactive enforcement, transparency, and a shared institutional commitment to compliance and continuous improvement.

Section 12: Guardrails for Data & Model Sharing and Dissemination

Purpose: To ensure that all data and AI model sharing—internally, externally, or publicly—adheres to UT Southwestern's ethical, legal, and governance standards.

12.1. Pre-Sharing Compliance Checklist

Before any dataset or AI model output is shared or disseminated:

- Confirm the dataset is **de-identified, aggregated, or synthetic** if PHI is involved.
- Verify the presence of **valid DUA or IRB protocol** for identifiable data.
- Ensure SNOMED CT and ICD coding standards have been applied where applicable.
- Classify the AI model and associated data under the appropriate **Risk Tier (Section 6)**.
- Check alignment with **AI Lifecycle Governance (Section 5)** and intended use.
- If unclear, escalate to the Data Governance Committee for adjudication.

12.2. Cross-Institutional and System-Wide Collaboration

- For any sharing with **UT System entities**, ensure alignment with the **UT REAL Health AI Initiative governance principles**.
- Validate compliance with internal **cross-site data governance policies**.
- Confirm presence of shared **research protocols and authorization logs**.

12.3. Public Dissemination Review

If data or AI model results are to be publicly shared (e.g., publications, conferences, media):

- Submit a **Public Dissemination Request Form (Section 2)**.
- Obtain approvals from:
  - **Legal Counsel**
  - **IRB (if human data is involved)**
  - **Data Governance Officer**
  - **Communications/PR Office** (for press, webinars, or public announcements)

12.4. Documentation and Auditability

- Every data or model sharing activity must be logged in the **Data Use Registry (Section 1)**.
- Record must include:
  - Dataset or model identifier
  - Project owner
  - Recipients and collaborators
  - Purpose and intended audience
  - Final approval signatures

12.5. Prohibited Practices

- Sharing of raw PHI without proper encryption or de-identification.
- Using institutional data to train commercial models without explicit DUA.
- Publicly disclosing model outputs that could infer private or sensitive information.

12.6. Enforcement

- Any non-compliant sharing or publication will trigger investigation under Section 11 (Enforcement).

This guardrail framework ensures responsible, secure, and transparent collaboration and public engagement around AI development and research at UT Southwestern.