Policy Document

Publication Date: October 01, 2025
Applicability: All Healthcare employees, contractors, and affiliates
Status: For Internal Use Only

1.0 Scope and Purpose

1.1 Purpose

This Firmwide Policy on Artificial Intelligence ("the Policy") establishes the governance framework for the design, development, procurement, deployment, and use of Artificial Intelligence ("AI") systems across Healthcare ("the Organization") in compliance with the Health Insurance Portability and Accountability Act (HIPAA).

The purpose of this Policy is to ensure that all AI systems — particularly those processing Protected Health Information (PHI) such as the Claim Reimbursement Agent — are developed and operated responsibly, ethically, and securely, in alignment with HIPAA's Privacy, Security, and Breach Notification Rules.

1.2 Scope

This Policy applies to all AI and AI-enabled systems used within [Healthcare] and its subsidiaries that collect, process, transmit, or store PHI. This includes but is not limited to:

- Clinical and administrative AI systems handling claims, reimbursements, or patient data.
- Generative and analytical AI models used in healthcare insights or documentation.
- AI agents developed internally or integrated from third-party vendors.

This Policy supplements existing frameworks including the Data Privacy and Security Policy, HIPAA Compliance Manual, Cybersecurity Policy, and Vendor Risk Management Policy.

1.3 Definitions

- **Protected Health Information (PHI):** Any individually identifiable health information held or transmitted by the Organization.
- **AI System Inventory:** A centralized register of all AI tools processing PHI.
- **AI Business Sponsor:** The responsible unit ensuring compliance of the AI system with HIPAA and organizational policies.
- **Claim Reimbursement Agent:** An AI-powered system designed to assist users in securely managing, submitting, and tracking healthcare reimbursement claims while

complying with HIPAA requirements.

2.0 Core Principles for HIPAA-Compliant and Trustworthy AI

All AI activities at Healthcare must follow the below principles:

- **Accountability:** Every AI system must have a designated AI Business Sponsor and documented lines of responsibility for HIPAA compliance.
- **Fairness and Integrity:** AI systems shall be tested to prevent discriminatory or biased outcomes that could affect patient or claim processing decisions.
- **Transparency and Explainability:** AI outputs must be explainable and traceable. For example, claim approval or denial decisions must include interpretable reasoning.
- **Security and Resilience:** AI systems must apply encryption, access control, and secure architecture to safeguard PHI from unauthorized use or disclosure.
- **Privacy and Data Governance:** AI must comply with HIPAA's Privacy Rule, ensuring PHI is accessed, used, and retained strictly for legitimate purposes.
- **Human Oversight:** Human review and override mechanisms must exist for all critical AI outputs, particularly those impacting healthcare claims or benefits.

3.0 Governance and Oversight

3.1 Artificial Intelligence Risk and Compliance Committee (AIRCC)

The AIRCC oversees all AI governance under HIPAA compliance. Its responsibilities include:

- Approving this Policy annually and maintaining HIPAA alignment.
- Reviewing and approving all AI systems processing PHI.
- Monitoring audit results, breach reports, and compliance gaps.
- Reporting to the Compliance and Risk Management Committee.

3.2 Model Risk and HIPAA Compliance Management (MRHCM) Group

- Maintains the AI System Inventory with PHI classification.
- Conducts HIPAA risk assessments and ensures encryption, anonymization, and de-identification controls are active.
- Validates AI model fairness, accuracy, and interpretability.
- Performs independent review of AI models affecting healthcare or reimbursement operations.

3.3 AI Business Sponsors

- Serve as the first line of defense for AI compliance.

- Ensure AI use aligns with HIPAA Privacy and Security Rules.
- Maintain auditable records of data usage and model decisions.
- Ensure that any third-party AI vendors sign a **Business Associate Agreement (BAA)** before processing PHI.

3.4 Control-Side Stakeholders

Legal, Compliance, IT Security, and Risk Management teams ensure:

- All AI systems undergo HIPAA risk assessments.
- Incident response, breach notification, and audit trails comply with federal and state privacy laws.

4.0 HIPAA-Aligned AI Risk Management Framework

4.1 AI System Inventory

All AI systems must be registered in the AI System Inventory, which includes:

- The nature of PHI handled.
- Encryption standards (AES-256, TLS 1.3).
- Data retention and access logging mechanisms.
- Business Associate details (if applicable).

4.2 Risk Categorization

AI systems are categorized by their impact on PHI confidentiality, integrity, and availability:

- **Prohibited Risk:** Any AI use that violates HIPAA or processes PHI without consent.
- **High Risk:** AI affecting patient claims, diagnosis, or treatment recommendations (e.g., Claim Reimbursement Agent).
- **Moderate Risk:** Internal analytics tools or anonymized datasets.
- **Low Risk:** Non-PHI-related automation (e.g., scheduling bots).

High-risk AI requires prior AIRCC approval, human review capability, and independent validation.

4.3 Risk Assessment

Each AI system must undergo a HIPAA risk assessment addressing:

- **Data Privacy Risks:** PHI protection, consent verification, de-identification.
- **Technical Risks:** Encryption, authentication, and secure data transmission.
- **Operational Risks:** Model explainability, accuracy, and audit logging.
- **Ethical Risks:** Bias or discriminatory outputs.

Mitigation actions must be completed before deployment.

5.0 Policy Requirements

5.1 AI Approval

No AI system may process PHI without prior approval by the AIRCC and MRHCM. Unauthorized deployments constitute a HIPAA violation.

5.2 Data Governance

- Only de-identified or minimum necessary PHI may be used for training.
- Data must comply with [Healthcare]'s HIPAA Privacy and Security Policies.
- Bias testing and data quality validation are mandatory.

5.3 Third-Party AI and Vendor Use

- Vendors must sign Business Associate Agreements (BAAs).
- Vendor systems must demonstrate HIPAA-compliant encryption and data isolation.
- Confidential data cannot be entered into public AI platforms (e.g., ChatGPT, Gemini).
- Approved vendors are reviewed annually for HIPAA adherence.

5.4 Continuous Monitoring

All production AI must be continuously monitored for:

- Security vulnerabilities and drift in model behavior.
- Unauthorized PHI access or export.
- Accuracy and fairness degradation.
- Incident logging and breach notifications (as per 45 CFR §164.308(a)(6)).

6.0 HIPAA-Compliant Use Case: Claim Reimbursement Agent

The **Claim Reimbursement Agent** is an AI-powered tool that automates and assists with healthcare reimbursement requests while adhering to HIPAA standards.

System Features

- **User Authentication:** Secure email login and session-based access control.
- **Document Upload & Encryption:** PHI-containing claim documents are encrypted (AES-256).
- **AI Analysis:** The agent analyzes claims while maintaining data minimization and audit trails.
- **Explainable Decisions:** Claim status and reasoning (approval, denial, resubmission) are visible and traceable.

- **AI Assistant:** A HIPAA-compliant conversational assistant provides policy guidance and clarifies claim decisions securely.

Compliance Controls

- **Access Logs:** Every action is timestamped and stored.
- **Audit Reports:** Available for compliance and insurance audits.
- **Data Retention:** PHI retained only as long as required by law.
- **Incident Management:** Breaches are immediately reported to the HIPAA Privacy Officer.

7.0 Reporting and Escalations

- The AIRCC shall report quarterly to the Enterprise Risk Committee on HIPAA-AI compliance posture.
- Violations are subject to investigation under the HIPAA Sanction Policy and Employee Conduct Policy.
- Exceptions require written approval from the AIRCC Chair and the Chief Compliance Officer.