# ISO/IEC 42001 Gap Analysis

ClearPath Pharmacy: AI Governance Portfolio

| Document information | Details |
|---|---|
| Organization | ClearPath Pharmacy: Specialty Pharmacy Services |
| Document title | ISO/IEC 42001:2023 Gap Analysis: AI Management System |
| Document ID | AI-ISO42001-001 |
| Classification | Confidential: Internal Use Only |
| Version | 1.0 |
| Effective date | May 18, 2026 |
| Next review date | May 18, 2027 |
| Prepared by | Information Security & Compliance Department |
| Approved by | Information Security Steering Committee |
| AI system in scope | Patient Adherence and Outreach Prioritization (AOP) tool |

## AI use case in scope

**System:** The Patient Adherence and Outreach Prioritization (AOP) tool, a third-party predictive analytics system supplied by MedSignal Analytics under a Business Associate Agreement. The system ingests patient data, predicts which patients are at risk of missing or stopping therapy, and ranks them so care staff know whom to contact first.

**Why this use case matters:** It processes protected health information, it influences decisions that affect patients (who receives outreach first), and adherence is a core clinical and business concern for a specialty pharmacy. That places it squarely at the intersection of HIPAA and AI governance.

**The HIPAA / AI overlap (the thread through every document):** Wherever the AOP tool processes PHI, HIPAA Privacy and Security Rule obligations apply alongside the AI governance work. Minimum necessary, a signed BAA, and access controls are AI governance controls and HIPAA controls at the same time.

## 1. Scope and Methodology

This gap analysis evaluates ClearPath Pharmacy against ISO/IEC 42001:2023, the AI management system (AIMS) standard, focused on the AOP tool. It mirrors the structure of ClearPath's existing NIST CSF 2.0 Gap Analysis so the two read as siblings. Each clause and key Annex A control is assessed for Requirement, Current State, Gap, Remediation, and Priority (High, Medium, Low). Priority legend: H = High, M = Medium, L = Low.

### Maturity at a glance

- Strong foundation: an AI Use Policy, a HIPAA program, an ISMS, and a security policy package already exist.
- Primary gaps: a formal AI management system, AI impact assessments, fairness and drift measurement, and lifecycle controls.

## 2. Clauses 4 to 10

| Clause / control | Requirement | Current state | Gap | Remediation | Pri. |
|---|---|---|---|---|---|
| 4 Context | Determine internal/external issues, interested parties, and AIMS scope. | Stakeholders informally understood; HIPAA scope defined. | No documented AIMS scope or interested-party analysis for AI. | Define and document AIMS scope and interested parties. | M |
| 5 Leadership | Top-management commitment, an AI policy, roles and responsibilities. | AI Use Policy approved by leadership; Steering Committee exists. | No AI policy objectives or assigned AIMS roles below policy level. | Assign AIMS roles; set measurable AI objectives. | H |
| 6 Planning | AI risk assessment and AI system impact assessment; objectives. | General risk culture; HIPAA risk assessment done. | No AI-specific risk or impact assessment methodology. | Adopt AI risk and impact assessment procedures. | H |
| 7 Support | Resources, competence, awareness, communication, documented information. | Security awareness training exists. | No AI-specific competence or awareness program; sparse AI documentation. | Add AI training; build a documented-informati | M |

| Clause / control | Requirement | Current state | Gap | Remediation | Pri. |
|---|---|---|---|---|---|
| | | | | on set for AI. | |
| 8 Operation | Operational planning and control; run the impact assessment. | Tool operating with vendor under BAA. | Operational AI controls not formalized; impact assessment not executed. | Operationalize controls; complete the impact assessment. | H |
| 9 Performance evaluation | Monitoring, measurement, internal audit, management review. | Security monitoring and audits exist. | No AI performance metrics, AI internal audit, or AI management review. | Define AI metrics; add AI to audit and management review. | H |
| 10 Improvement | Nonconformity, corrective action, continual improvement. | Corrective action exists for security. | No AI nonconformity or corrective-action loop. | Extend corrective-action process to cover AI. | M |

## 3. Annex A Controls (most relevant)

| Clause / control | Requirement | Current state | Gap | Remediation | Pri. |
|---|---|---|---|---|---|
| A.2 AI policy | Establish and maintain an AI policy. | POL-AI-001 in place. | Policy lacks objectives, metrics, and review evidence. | Add objectives and review cadence to the policy. | M |
| A.3 Roles | Define AI roles and responsibilities. | Policy assigns high-level oversight. | No named AOP system owner or AI committee. | Name owner; charter AI governance committee. | H |
| A.4 Resources | Document data, tooling, and human resources for AI. | Vendor and tool known. | Data and model resources not documented. | Maintain an AI system and | M |

| Clause / control | Requirement | Current state | Gap | Remediation | Pri. |
|---|---|---|---|---|---|
| | | | | data inventory. | |
| A.5 Impact assessment | Assess AI system impacts on individuals and society. | Not performed. | No AI impact assessment for the AOP tool. | Complete and retain an AI impact assessment. | H |
| A.6 Lifecycle | Manage the AI system across its lifecycle. | Operating phase only is managed informally. | No lifecycle controls (design, deployment, retirement, change). | Define lifecycle and change-management controls. | M |
| A.7 Data for AI | Govern data quality and provenance for AI. | PHI governed under HIPAA. | No documented data quality or provenance checks for the model. | Add data quality and provenance requirements. | M |
| A.10 Third parties | Manage suppliers and third-party AI. | BAA signed with vendor. | No AI-specific supplier obligations or monitoring. | Add AI clauses and supplier monitoring. | H |

# 4. Top Gaps and Phased Remediation Roadmap

## Phase 1 (0 to 3 months): Governance foundation

- ☐ Name an AOP system owner and charter the AI governance committee (5, A.3).
- ☐ Set AI policy objectives and review cadence (5, A.2).

## Phase 2 (3 to 6 months): Assessment and measurement

- ☐ Complete the AI impact assessment and AI risk assessment (6, 8, A.5).
- ☐ Define AI performance, fairness, and drift metrics (9).

## Phase 3 (6 to 12 months): Operate and improve

- ☐ Add AI to internal audit, management review, and corrective action (9, 10).

☐ Add AI clauses and supplier monitoring at vendor renewal (A.10).