AI GOVERNANCE EXECUTIVE GUIDE SERIES • VOLUME 2

AI Governance for Healthcare

Clinical AI Safety, FDA Compliance, and Patient Protection

A Comprehensive Guide for FDA SaMD Alignment, HIPAA Compliance, and Enterprise Clinical AI Risk Management

Version 1.0 • December 2025
Prepared by FERZ LLC
ferz.ai

Governance is the authorization boundary: the point where outputs become decisions, and where evidence—not explanations—must exist.

FOR

Chief Medical Officers • Chief Information Officers • Heads of Clinical AI

Compliance Officers • Clinical Informaticists • Quality & Patient Safety Officers

License and Terms of Use

Copyright & License

This work is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0). You are free to share (copy and redistribute the material in any medium or format) and adapt (remix, transform, and build upon the material for any purpose, including commercial purposes) under the following terms:

- **Attribution:** You must give appropriate credit, provide a link to the license, and indicate if changes were made. Attribution must not suggest endorsement by the licensor.

The full license text is available at: creativecommons.org/licenses/by/4.0

Attribution Guidance

When citing or reusing this work, attribution must include:

> FERZ LLC, "AI Governance Executive Guide: Healthcare," 2025. Available at ferz.ai.

If the material is modified, adapted, or excerpted, the attribution must clearly indicate that changes were made.

Commercial Scope Notice

This publication is provided as a public reference framework for AI governance and risk management.

While reuse and adaptation are permitted under the CC BY 4.0 license, commercial services, tooling, certification programs, managed governance platforms, and implementation accelerators derived from this framework are offered separately by FERZ LLC or its authorized partners.

This notice does not restrict rights granted under the license; it clarifies the separation between open reference material and commercial offerings.

No Warranty or Endorsement

This document is provided "as is," without warranties of any kind, express or implied.

Use of this framework does not constitute regulatory, legal, or compliance advice, nor does it imply endorsement by FERZ LLC of any implementation, product, or service that references it.

Canonical Reference

The authoritative version of this document is maintained by FERZ LLC. Subsequent adaptations or derivatives should reference the original source to ensure conceptual fidelity and version traceability.

Executive At-a-Glance

Audience

Chief Medical Officers, Chief Information Officers, Heads of Clinical AI, Compliance Officers, Clinical Informaticists, and Quality & Patient Safety Officers at health systems, hospitals, medical device manufacturers, and healthcare technology companies.

Core Thesis

> Governance is the authorization boundary: the point where outputs become decisions, and where evidence—not explanations—must exist.

Two Governance Tracks

Track	Primary Risk	Ownership
Decisioning AI	Clinical risk (FDA SaMD, patient safety)	Clinical Governance / Quality
Communications AI	Records/privacy (HIPAA, state laws)	Compliance / Privacy Office

Four-Tier Classification

Tier	Risk Level	Governance Intensity
Tier 1	Critical	Full validation: clinical testing, FDA pathway, quality committee approval
Tier 2	Elevated	Proportionate: validation, annual review, clinician oversight
Tier 3	Standard	Operational controls, data security, HIPAA compliance
Tier 4	Minimal	Acceptable use policy only

90-Day Implementation

- **Weeks 1–4 (Foundation):** Clinical AI inventory sweep, gap assessment, tiering criteria, governance structure
- **Weeks 5–8 (Critical Systems):** Tier 1 focus, FDA/safety gap analysis, bias testing, validation approach
- **Weeks 9–12 (Operationalization):** Policy deployment, training, Examiner Pack compilation, mock survey

Maturity Endpoint

Level 5: Cryptographically Verifiable — every clinical AI action produces an evidence-grade artifact that answers "how do you know?" with mathematical certainty.

 •

Executive Summary

Healthcare organizations face a convergence challenge: AI and machine learning systems now directly influence clinical decisions, yet existing quality and safety frameworks—designed for traditional medical devices and clinical processes—require substantial extension to address the unique characteristics of modern AI systems.

The gap is significant. FDA guidance on AI/ML-based Software as a Medical Device (SaMD) provides a foundation, but the agency is still developing its approach to continuously learning systems. HIPAA addresses data privacy but not algorithmic decision-making. The Joint Commission evaluates quality systems but has limited AI-specific standards. Organizations must interpret and extend these frameworks themselves.

This creates both risk and opportunity. Organizations that proactively extend their clinical governance frameworks to address AI gain regulatory credibility, reduce patient safety risk, and establish operational advantages. Those that wait face increasing scrutiny, potential adverse events, and competitive disadvantage as AI becomes standard of care.

Two Governance Tracks

AI governance in healthcare operates across two distinct tracks, each with different regulatory drivers and organizational ownership:

Track	Primary Risk	Key Regulations	Typical Ownership
Decisioning AI	Clinical / patient safety	FDA SaMD, 21 CFR 820, State practice acts	Clinical Governance / CMO
Communications AI	Privacy / records	HIPAA, 21 CFR Part 11, State privacy laws	Compliance / Privacy Office

Decisioning AI: Clinical decision support, diagnostic AI, treatment recommendations, risk stratification, resource allocation, triage prioritization. Governed primarily through clinical validation, FDA pathways, and patient safety frameworks.

Communications AI: Patient communication drafts, clinician copilots, discharge summaries, prior authorization assistance, adverse event reporting, clinical documentation. Governed primarily through HIPAA, medical records requirements, and professional standards.

While communications AI may not directly execute clinical decisions, its regulatory risk profile can be equal or higher due to HIPAA, medical records integrity, professional liability, and patient trust exposure. Do not assume that communications use cases are inherently lower risk than decisioning use cases.

This distinction matters because surveyors and regulators ask different questions, and internal ownership often differs. A single AI system may span both tracks—a clinician copilot that drafts clinical notes (records) based on diagnostic analysis (clinical)—requiring coordinated governance.

The Core Challenge

Healthcare AI governance has three pillars: Development, Validation, and Governance. Each requires extension for AI:

Pillar	Traditional Approach	AI/ML Extension Required
Development	Device design controls, clinical protocols	Training data provenance, algorithm selection, bias assessment, explainability approach

Pillar	Traditional Approach	AI/ML Extension Required
Validation	Clinical trials, bench testing	Demographic subgroup testing, drift monitoring, adversarial robustness, real-world performance
Governance	Quality committees, credentialing	Expanded inventory (embedded AI, vendor), new risk categories, continuous monitoring

What This Guide Provides

- **Regulatory mapping:** How FDA SaMD guidance, HIPAA, CMS requirements, and EU AI Act apply to clinical AI systems
- **Risk framework:** Four-tier classification system with explicit Tier 1 triggers to prevent governance arbitrage
- **Governance structure:** Clinical governance model extended for AI oversight
- **Lifecycle management:** Development, validation, deployment, monitoring, and retirement processes
- **Survey readiness:** Documentation standards, Examiner Pack template, and response playbooks
- **GenAI controls:** Dedicated control set for generative AI including hallucination, documentation integrity, and disclosure
- **Board metrics:** KRIs/KPIs for executive clinical AI reporting
- **Implementation roadmap:** 90-day plan with maturity progression to cryptographically verifiable governance

90-Day Implementation Overview

Phase	Key Deliverables
Weeks 1-4 Foundation	Clinical AI system inventory sweep, existing framework gap assessment, tiering criteria established, core policies drafted, governance structure defined
Weeks 5-8 Critical Systems	Tier 1 systems identified and prioritized, gap analysis against FDA requirements, bias testing for diagnostic/treatment AI, validation approach documented, monitoring capabilities established
Weeks 9-12 Operationalization	Policies approved and deployed, training completed, shadow AI detection active, Tier 1 documentation packages compiled, mock survey conducted

PART I

The Regulatory Landscape

Chapter 1: Existing Frameworks That Apply Today

Healthcare organizations do not operate in a regulatory vacuum when deploying AI. Multiple existing frameworks apply, even in the absence of comprehensive AI-specific regulation. Understanding these frameworks—and how regulators are extending them to AI—is essential for defensible governance.

FDA AI/ML Guidance: The Foundation

The FDA has issued guidance on AI/ML-based Software as a Medical Device (SaMD), establishing expectations for AI systems that meet the definition of a medical device. While still evolving, this guidance provides the foundation for clinical AI governance.

> **Key Principle:** FDA defines SaMD as software intended to be used for medical purposes without being part of a hardware medical device. AI systems that diagnose, treat, cure, mitigate, or prevent disease may meet this definition regardless of whether they are marketed as 'decision support.'

The FDA's Total Product Lifecycle Approach

1. Good Machine Learning Practice (GMLP): FDA has endorsed principles for GMLP including multi-disciplinary expertise, representative data, independent datasets, reference standards, model design tailored to data, focus on human-AI team performance, clinical study testing, user information transparency, monitoring of deployed models, and cybersecurity safeguards.

2. Predetermined Change Control Plans (PCCP): For AI/ML devices that learn and adapt, FDA is developing a framework for manufacturers to pre-specify types of changes that would not require new submissions, enabling continuous improvement while maintaining safety.

Risk Classification for SaMD

FDA uses a risk-based framework from the International Medical Device Regulators Forum (IMDRF):

- State of healthcare situation: Critical, Serious, or Non-serious
- Significance of information: Treat/diagnose, Drive clinical management, or Inform clinical management

Higher-risk combinations require more rigorous validation and regulatory pathway (510(k), De Novo, PMA).

The boundary between regulated SaMD and exempt clinical decision support (CDS) is nuanced. FDA provides exemptions for certain CDS that displays information for clinician review without providing specific recommendations. However, exemptions have specific constraints, and many AI systems do not qualify. When regulatory status is ambiguous, treat the system as Tier 1 until formal determination is obtained.

21 CFR Part 11: Electronic Records

21 CFR Part 11 establishes requirements for electronic records and signatures in FDA-regulated industries. For clinical AI, this means:

 •

- **Audit trails:** Complete, timestamped records of system actions and changes
- **Access controls:** Role-based permissions with authentication
- **Data integrity:** Prevention of unauthorized modifications
- **Electronic signatures:** Legally binding sign-offs for approvals

HIPAA: Privacy and Security

HIPAA's Privacy and Security Rules apply to AI systems that process protected health information (PHI):

- **Minimum necessary:** AI systems should access only the PHI required for their function
- **Business Associate Agreements:** Third-party AI vendors must sign BAAs
- **Security safeguards:** Technical, administrative, and physical protections for PHI in AI systems
- **Breach notification:** AI-related breaches trigger HIPAA notification requirements

CMS Conditions of Participation

Hospitals participating in Medicare/Medicaid must meet CMS Conditions of Participation, which increasingly implicate AI:

- **Quality Assessment and Performance Improvement (QAPI):** AI systems affecting patient outcomes fall under QAPI oversight
- **Medical staff credentialing:** Clinicians using AI may need competency documentation
- **Patient rights:** Patients may have rights to information about AI use in their care

The Joint Commission

Joint Commission standards for accredited organizations increasingly apply to clinical AI:

- **Leadership standards:** Oversight of technology affecting patient care
- **Performance improvement:** Monitoring and improving AI system performance
- **Information management:** Integrity of clinical information including AI outputs

State Medical Practice Acts

State medical boards regulate the practice of medicine, which may include AI-assisted clinical decisions:

- AI may not independently practice medicine without licensed clinician oversight
- Clinicians remain responsible for AI-informed decisions
- Some states are developing specific AI guidance for practitioners

The standard of care remains the clinician's responsibility. Use of AI does not shift the duty of care from the clinician to the technology or vendor. Clinicians must exercise independent professional judgment, and AI outputs should inform—not replace—clinical decision-making.

Chapter 2: What's Coming

The regulatory landscape for AI in healthcare is evolving rapidly. Organizations should anticipate and prepare for emerging requirements rather than waiting for final rules.

EU AI Act: Extraterritorial Impact

The EU AI Act, with enforcement beginning in August 2025, has extraterritorial reach affecting U.S. healthcare organizations that serve EU patients or deploy AI systems whose outputs are used in the EU.

High-risk classification: Medical devices and in vitro diagnostic devices are explicitly classified as high-risk AI, requiring conformity assessments, risk management systems, data governance, technical documentation, human oversight, accuracy/robustness requirements, and registration.

Anticipated U.S. Regulatory Evolution

While the specific regulatory trajectory depends on administration priorities, several developments are likely:

- **FDA AI/ML Action Plan:** Continued development of the Total Product Lifecycle approach and PCCP framework
- **HIPAA updates:** Potential modernization to address AI and advanced analytics
- **ONC Health IT certification:** AI-specific certification criteria for EHR-embedded algorithms
- **CMS payment policy:** Reimbursement considerations for AI-assisted care
- **State legislation:** Growing state-level AI transparency and accountability requirements

Importantly, supervisory expectations often evolve through survey practice and enforcement actions before formal rulemaking occurs. Organizations should not wait for explicit AI regulation to implement governance frameworks.

 •

PART II

Risk Framework for Healthcare AI

Chapter 3: AI System Classification

Expanding the Clinical AI Inventory

The first challenge in AI governance is defining what counts as a "clinical AI system" subject to governance. Traditional inventories focused on formal medical devices. AI governance requires expanding scope significantly.

For governance purposes, any system that materially influences clinical decisions, patient care, or regulated communications is treated as subject to governance, regardless of technical implementation. This avoids definitional debates that delay governance while risk accumulates.

What counts as a clinical AI system:

- **Diagnostic AI:** Radiology interpretation, pathology analysis, symptom checkers, risk prediction
- **Treatment AI:** Clinical decision support, drug interaction checking, dosing recommendations, care pathway optimization
- **Operational AI:** Triage prioritization, resource allocation, scheduling optimization, readmission prediction
- **Generative AI:** Clinical documentation, patient communication, prior authorization, discharge instructions
- **Embedded AI:** AI features within EHRs, medical devices, monitoring systems, and vendor platforms
- **Third-party AI services:** APIs, cloud services, remote interpretation, outsourced analytics

The Four-Tier Framework

Healthcare AI governance requires a four-tier system that calibrates oversight intensity to patient safety risk. This framework aligns with FDA's risk-based approach while extending to non-device AI.

Tier	Criteria	Examples	Regulatory Touchpoints
Tier 1 Critical	Direct patient impact, diagnostic/treatment decisions, safety-critical	Diagnostic imaging AI, sepsis prediction, treatment recommendations, surgical robotics	FDA SaMD, 21 CFR 820, clinical validation, EU AI Act high-risk
Tier 2 Elevated	Clinical workflow impact, patient-facing with clinician review	Triage prioritization, readmission risk, clinical documentation assist	HIPAA, CMS quality reporting, medical records integrity
Tier 3 Standard	Operational efficiency, no direct patient decisions	Scheduling optimization, supply forecasting, staff allocation	Operational controls, data security
Tier 4 Minimal	Personal productivity, no PHI, no clinical context	General research, administrative drafting, education	Acceptable use policy only

Automatic Tier 1 Triggers

 •

Tiering frameworks fail when departments "tier down" to avoid validation overhead. To prevent governance arbitrage, the following conditions automatically classify a system as Tier 1, regardless of other assessments:

AUTOMATIC TIER 1 TRIGGERS

1. Impacts clinical decisions, diagnosis, treatment recommendations, or patient safety
2. Drives or materially influences quality reporting (CMS measures, Joint Commission, Leapfrog)
3. Produces outputs that become part of the medical record (even if "clinician reviewed")
4. Involves protected health information in clinical decisioning logic
5. Feeds into patient safety or clinical quality calculations

Third-Party Clinical AI Risk

Third-party clinical AI presents unique governance challenges. Organizations remain responsible for the safety and effectiveness of AI they deploy, regardless of vendor claims.

Vendor Minimum Evidence Package

To make third-party oversight actionable, require the following evidence from vendors, scaled by tier:

Evidence Required	Tier 1	Tier 2	Tier 3
Regulatory status / clearance documentation	Required	Required	Requested
Intended use statement and contraindications	Required	Required	Requested
Training data demographics and representativeness	Required	Required	N/A
Clinical validation study results	Required	Required	N/A
Bias testing across demographic subgroups	Required	Risk-based	N/A
Post-market surveillance data / incident history	Required	Required	Requested
BAA and audit cooperation language	Required	Required	Required

This is the difference between "we have vendor risk policy" and "we can survive a survey."

 •

Chapter 4: AI-Specific Risk Categories

Clinical AI systems present risk categories that extend beyond traditional medical device risk. Effective governance requires understanding and addressing each category.

Clinical Risk (Extended)

Training Data Risk: AI model quality depends fundamentally on training data. Risks include non-representative patient populations leading to biased performance, historical data encoding past disparities, data from different clinical settings not generalizing, and incomplete documentation of data provenance.

Diagnostic/Prognostic Risk: AI may produce false positives leading to unnecessary interventions or false negatives leading to missed diagnoses. Performance may vary across patient subgroups.

Drift Risk: Clinical AI can degrade over time as patient populations change, practice patterns evolve, or EHR documentation practices shift. Both data drift and concept drift require detection and remediation.

Explainability Risk: Clinicians may be unable to assess AI recommendations without understanding the reasoning. "Black box" AI may undermine clinical judgment and informed consent.

Operational Risk

- **Workflow integration failures:** AI systems failing to integrate properly with clinical workflows
- **Alert fatigue:** Excessive AI alerts leading to clinician desensitization
- **Latency and availability:** AI not meeting performance requirements for time-sensitive clinical decisions
- **Rollback capabilities:** Inability to quickly revert to non-AI workflows when issues arise

Compliance Risk

- **HIPAA violations:** Unauthorized access to or disclosure of PHI through AI systems
- **Medical records integrity:** AI-generated content compromising record accuracy or completeness
- **Professional liability:** Clinician responsibility for AI-informed decisions
- **Informed consent:** Patient rights to know about AI involvement in their care

Cybersecurity and Data Risk

- **Training data poisoning:** Adversaries corrupting training data to influence clinical AI behavior
- **Adversarial attacks:** Inputs crafted to cause AI misclassification (e.g., adversarial images)
- **PHI leakage:** Sensitive information exposed through AI outputs or model inversion
- **Prompt injection:** Manipulating generative AI through crafted inputs to bypass safety rails

Chapter 5: Generative AI Controls

Generative AI presents unique control requirements beyond traditional clinical AI governance. Because GenAI can produce novel outputs—clinical notes, patient communications, discharge instructions—that may enter the medical record or influence care, a dedicated control set is required.

Data Security Controls

- **PHI input filtering:** Prevent unnecessary PHI from entering GenAI prompts; apply minimum necessary principles
- **Output monitoring:** Detect and prevent PHI leakage or hallucinated patient information in outputs
- **Prompt injection defense:** Technical controls against manipulation attempts that could generate harmful clinical content
- **Session isolation:** Ensure user sessions don't leak patient information across conversations

Clinical Documentation Controls

For AI-generated clinical documentation, medical records integrity requirements apply:

- **Draft retention:** Capture AI-generated drafts as well as final documentation
- **Clinician attestation:** Require explicit clinician review and sign-off before documentation enters the record
- **Authorship indication:** Clear indication when AI assisted in generating documentation
- **Hallucination detection:** Processes to identify fabricated clinical details (medications, allergies, history)

Use Case Governance

Category	Examples	Required Controls
Approved	Literature summarization, education, research drafts	Acceptable use acknowledgment, no PHI
Restricted	Clinical note drafts, patient message drafts, discharge instructions	Clinician review, documentation, approval workflow
Prohibited	Autonomous diagnosis, unreviewed patient communications, treatment decisions	Technical enforcement, exception process only

Hallucination and Accuracy Controls

Generative AI may produce plausible but incorrect clinical content. Specific controls include:

- Explicit warnings that AI-generated content must be verified
- Structured output validation against EHR data where possible
- Sampling and audit processes for AI-generated documentation
- Incident reporting for identified hallucinations with clinical impact

Human Approval Requirements

Define approval gates for clinical GenAI outputs:

- All clinical documentation requires clinician review and attestation before entry to medical record

 •

- Patient-facing communications require clinician approval before sending
- Prior authorization content requires appropriate clinical sign-off
- Adverse event reports require qualified reviewer approval

Human review must be meaningful, not rubber-stamp. Reviewers must have the authority, training, and time to override or block AI outputs. Checkbox acknowledgments without substantive review do not satisfy clinical oversight requirements.

PART III

Governance Structure

Chapter 6: Organizational Model

Clinical AI Governance Structure

Healthcare organizations operate under quality and safety governance structures. AI governance must integrate into these structures rather than creating parallel governance.

Function	Traditional Role	AI Governance Extension
Clinical Departments (First Line)	Own clinical quality and safety in daily operations	AI system ownership, use case documentation, performance monitoring, incident reporting, clinician training
Quality & Compliance (Second Line)	Set policy, monitor quality, independent review	AI policy and standards, independent validation coordination, inventory management, regulatory liaison
Internal Audit (Third Line)	Independent assurance of framework effectiveness	AI governance framework audits, control testing, compliance verification, AI-specific audit techniques

Key Roles

Chief Medical Officer / Chief Medical Informatics Officer: Executive accountability for clinical AI safety and effectiveness

Clinical AI Governance Lead: Dedicated focus on AI-specific clinical oversight, bias monitoring, and validation coordination

Clinical AI Validation Team: Specialized validation capability with skills in clinical testing, demographic subgroup analysis, and performance monitoring

Department AI Champions: Clinician leads who understand both clinical context and AI capabilities in their specialty

Governance Bodies

Medical Executive Committee: Ultimate clinical oversight of Tier 1 AI deployments; charter should explicitly include AI

Clinical AI Subcommittee: Working body that reviews AI use cases, validation results, and monitoring data; reports to MEC

Pharmacy & Therapeutics (for drug-related AI): Oversight of AI affecting medication decisions

Health IT Steering Committee: Technical and operational oversight of AI implementations

Governance Authority and Capability Requirements

Clinical AI governance frameworks fail in two predictable ways: the governance function lacks authority to enforce standards, or it lacks competence to make credible decisions. Both failure modes must be addressed by design.

 •

The Authority Problem

Governance without authority produces policy documents that IT ignores and clinical departments route around. Effective clinical AI governance requires:

- **Pipeline integration:** Governance must have hooks into actual deployment processes—intake forms that trigger before vendor contracts, validation gates that block EHR integration, monitoring access with real clinical performance data. Policy without pipeline integration is theater.
- **Escalation path with teeth:** When governance raises patient safety concerns, there must be an escalation path to someone who can override IT delivery pressure and departmental adoption pressure. This typically means reporting to the CMO, a Board Quality Committee, or having direct access to the CEO on material patient safety issues.
- **Information rights:** Even where governance cannot block deployments, it must have visibility into all clinical AI systems. Shadow AI in clinical workflows is a governance design failure, not just a clinician behavior problem. Information rights include: access to Health IT inventories, vendor contract notifications, EHR integration logs, and clinical decision support configurations.
- **Budget independence:** Governance cannot depend on the goodwill of functions it oversees. Validation resources, monitoring tools, and external clinical expertise must be funded independently of IT or departmental budgets.

The Competence Problem

Authority without competence produces either rubber-stamp approvals (governance theater) or reflexive blocking (innovation killing). Neither serves patients. Effective clinical AI governance requires dual competency:

- **Clinical/regulatory expertise:** Deep understanding of FDA pathways, HIPAA, clinical workflow integration, and patient safety frameworks. Ability to translate regulatory requirements into operational controls that clinicians will actually follow.
- **Technical credibility:** Sufficient understanding of AI/ML to evaluate vendor validation claims, assess demographic bias testing, and recognize when technical teams are deflecting or oversimplifying. This does not require the governance lead to be a data scientist, but they must be able to hold their own in technical discussions with vendors and informatics teams.

In practice, this dual competency usually requires a team rather than a single individual—often pairing clinical informaticists with quality/regulatory specialists under unified governance leadership. The CMIO role, where it exists, sometimes bridges these domains.

Reporting Line Tradeoffs

Where the clinical AI governance function reports determines its capture risk:

Reports To	Advantage	Capture Risk
CMO / Chief Medical Officer	Clinical authority, patient safety mandate	May lack technical access; dependent on IT cooperation
CIO / CMIO	Technical access, EHR integration easier	Captured by implementation pressure; asked to approve what's already contracted
CNO / Clinical Departments	Clinical workflow context, adoption focus	Captured by departmental pressure; governance becomes checkbox
Compliance / Legal	Regulatory credibility, independence	May lack clinical and technical depth; legalistic rather than operational
CEO / Board Quality Committee	Maximum independence and authority	May lack day-to-day clinical connection; reserved for largest systems

 •

The most effective structures typically have clinical AI governance reporting to the CMO with a strong dotted line to the CIO/CMIO for technical liaison, or embedded within an empowered Quality function with direct Board Quality Committee access for Tier 1 patient safety escalations.

The 'Effective Challenge' Test

Effective governance requires critical analysis by objective, informed parties. For clinical AI governance, apply this test to your organizational design:

- Can your governance function say 'no' to a Tier 1 clinical AI deployment that a department chair wants to launch?
- Can your governance function obtain validation data that a vendor doesn't want to provide?
- Does your governance function learn about clinical AI initiatives before the vendor contract is signed, or after go-live?
- Can your governance function compel remediation of patient safety findings, or only recommend?
- Does your governance function have the clinical and technical vocabulary to challenge vendor performance claims?

If the answer to any of these is 'no,' your governance structure has a design flaw that will manifest during a survey, an FDA inspection, or a patient safety event.

Chapter 7: Policy Framework

Effective AI governance requires a comprehensive policy framework that provides clear guidance while remaining flexible enough to accommodate evolving AI capabilities.

Core Policies Required

1. Clinical AI Acceptable Use Policy

- Permitted uses by role and clinical context
- Prohibited uses (autonomous diagnosis, unreviewed patient communications)
- Shadow AI prohibition—no unapproved AI in clinical workflows
- PHI handling requirements in AI systems

2. Clinical AI Development/Acquisition Policy

- Development lifecycle requirements by tier
- Documentation standards (training data, validation approach, intended use)
- Testing and validation gates before clinical deployment
- Vendor due diligence requirements

3. Clinical AI Validation Policy

- Validation scope and frequency by tier
- Validation techniques (clinical accuracy, demographic subgroup testing, real-world performance)
- Independence requirements for validation
- Findings classification and remediation timelines

4. Clinical AI Monitoring Policy

- Continuous monitoring requirements (performance metrics, drift detection)
- Periodic review cadence by tier
- Escalation triggers and clinical incident reporting
- Post-market surveillance procedures

5. Third-Party Clinical AI Policy

- Due diligence requirements before contracting
- Minimum evidence package by tier
- Ongoing performance monitoring
- Incident notification and cooperation requirements

PART IV

Lifecycle Management

Chapter 8: Development and Validation

Pre-Development Requirements

Before clinical AI development or acquisition begins, several assessments should be completed:

- **Clinical use case justification:** Clear articulation of clinical problem and why AI is appropriate
- **Intended use statement:** Specific clinical context, user, and decision support function
- **Patient population definition:** Who will this AI be used for, and is training data representative
- **Regulatory pathway assessment:** Determination of FDA classification and requirements
- **Ethical review:** For Tier 1/2 systems, assessment of potential bias and equity concerns

Development Documentation Standards

Clinical AI development requires thorough documentation aligned with FDA expectations:

- **Training data specification:** Source, patient demographics, selection criteria, preprocessing, known limitations
- **Algorithm documentation:** Architecture selection rationale, alternatives considered, hyperparameter choices
- **Clinical endpoint definition:** What the AI is predicting/classifying and how ground truth was established
- **Performance characterization:** Sensitivity, specificity, PPV, NPV across relevant subgroups
- **Intended use and indications:** Specific clinical context, user qualifications, contraindications

Validation Framework

Validation requirements vary by tier:

Validation Activity	Tier 1	Tier 2	Tier 3	Tier 4
Clinical accuracy testing	Required	Required	N/A	N/A
Demographic subgroup analysis	Required	Risk-based	N/A	N/A
Local validation on site data	Required	Required	Recommended	N/A
Workflow usability testing	Required	Required	Basic	N/A
Independent clinical review	Required	Required	Self-assess	N/A

Chapter 9: Deployment and Monitoring

Deployment Controls

- **Staged rollout:** Phased clinical deployment with monitoring gates before full implementation
- **Rollback procedures:** Documented ability to revert to non-AI clinical workflows quickly
- **Performance baseline:** Establish baseline metrics before deployment for comparison
- **Clinician training:** Ensure users understand AI capabilities, limitations, and appropriate use
- **Patient notification:** Determine requirements for informing patients about AI use in their care

Patient notification requirements are risk- and jurisdiction-dependent. For Tier 1 decisioning AI (diagnostic, treatment, prognostic), involve legal counsel and ethics/consent governance to determine appropriate disclosure. Some states and payers are developing specific AI disclosure requirements.

Ongoing Monitoring

Review Type	Tier 1	Tier 2	Tier 3	Tier 4
Performance monitoring	Continuous	Monthly	Quarterly	N/A
Demographic subgroup review	Quarterly	Annual	N/A	N/A
Full revalidation	Annual	18 months	As needed	N/A
Clinical incident review	Within 24h	Within 72h	As needed	N/A

Audit Trails: Logs vs. Evidence

A critical distinction exists between operational logging and evidence-grade artifacts:

Concept	Definition	Regulatory Value
Logs	Operational trace of system activity—timestamps, user actions, errors, performance metrics	Necessary but not sufficient; can show "what happened" but not "why it was clinically appropriate"
Evidence-Grade Artifacts	Replayable, version-bound, policy-bound decision records with cryptographic integrity	Independently verifiable; can answer "how do you know?" for surveyors, FDA, malpractice defense

For Tier 1 clinical systems, the goal is to move beyond "audit logging enabled" toward evidence-grade artifacts that contain: immutable clinical decision records, algorithm version identifiers, input/output data hashes, clinical policy alignment, clinician attestation, and replay instructions. This distinction becomes critical at maturity Level 5.

PART V

Survey and Examination Readiness

Chapter 10: Documentation Standards

Clinical AI Documentation Package (Tier 1)

Each Tier 1 clinical AI system should have a complete documentation package containing:

- System identification (unique ID, clinical owner, vendor/developer, tier rationale)
- Clinical context (use case, workflow integration, patient population, clinical decisions affected)
- Technical documentation (algorithm, training data, performance characteristics)
- Validation documentation (scope, clinical testing results, subgroup analysis, limitations)
- Monitoring documentation (metrics, thresholds, escalation procedures, incident history)

Examiner Pack: Standard Binder Structure

For each Tier 1 clinical AI, maintain a ready-reference binder to minimize scrambling during surveys or inspections:

Tab	Contents
1	Inventory entry + tier classification rationale + regulatory status
2	Intended use statement + patient population + clinical workflow
3	Validation summary with clinical testing results and sign-offs
4	Performance monitoring dashboard + thresholds + last 3 months data
5	Change log / version history / algorithm updates
6	Clinical incidents + patient safety events + corrective actions
7	Vendor artifacts (if applicable): FDA clearance, validation studies, BAA

Chapter 11: Survey and Inspection Preparation

Common Survey/Inspection Questions

Prepare responses to common surveyor and inspector inquiries:

Inventory & Governance

- "Show me your complete clinical AI inventory"
- "How do you identify shadow AI in clinical workflows?"
- "Walk me through your clinical risk tiering methodology"
- "Who has authority to approve Tier 1 clinical AI?"

Validation & Safety

- "Show me validation documentation for [specific AI system]"
- "How do you test for demographic bias in diagnostic AI?"
- "What's your approach to ensuring AI works for your patient population?"
- "How do you validate vendor AI claims before deployment?"

Monitoring & Incidents

- "Show me evidence of ongoing performance monitoring"
- "What triggers a clinical AI safety review?"
- "Walk me through a recent AI-related patient safety event"
- "How do you detect when AI performance degrades?"

Survey Response Playbook

Documentation retrieval: Know where all clinical AI documentation lives and who can access it

Subject matter experts: Pre-identify clinical and technical SMEs for each Tier 1 system

Response coordination: Designate survey coordinator to manage requests

Issue escalation: Define escalation path for unexpected findings

Chapter 12: Board and Executive Reporting

Clinical AI Governance KRIs/KPIs

Executives adopt what they can track. The following metrics support board-level clinical AI governance reporting:

Metric	Definition	Target
Inventory coverage	% of known clinical AI use cases tiered and documented	>95%
Tier 1 validation currency	% of Tier 1 AI with current validation (<12 months)	100%
Performance alerts	Count of performance degradation alerts by severity	Trending ↓
Demographic disparity findings	Count of significant subgroup performance gaps	Zero unresolved
Vendor concentration	% of Tier 1 AI from single vendor	<40%
Shadow AI detections	Count of unapproved clinical AI discovered	Trending ↓
Patient safety events	AI-related patient safety events by severity	Zero serious
Time-to-remediate	Average days from finding to resolution by severity	<7 days for critical

Report these metrics quarterly to the Clinical AI Subcommittee and annually (with trends) to the Medical Executive Committee and Board Quality Committee.

PART VI

Implementation Roadmap

Chapter 13: 90-Day Implementation Plan

Phase 1: Foundation (Weeks 1-4)

Week 1-2: Inventory & Gap Assessment

- Conduct clinical AI system inventory sweep across all departments
- Map existing quality/safety frameworks to clinical AI requirements
- Identify policy and governance gaps
- Assess organizational readiness (clinical informatics, vendor management)

Week 3-4: Governance Structure

- Establish Clinical AI Subcommittee or expand existing committee charter
- Define roles and responsibilities
- Establish tiering criteria including automatic Tier 1 triggers
- Draft core policies

Phase 2: Critical Systems (Weeks 5-8)

Week 5-6: Tier 1 System Focus

- Identify and prioritize Tier 1 clinical AI systems
- Conduct gap analysis against FDA/clinical validation requirements
- Develop remediation plans
- Begin enhanced documentation

Week 7-8: Validation Enhancement

- Implement demographic subgroup testing for diagnostic/treatment AI
- Establish clinical performance monitoring
- Enhance drift detection capabilities
- Compile vendor minimum evidence packages

Phase 3: Operationalization (Weeks 9-12)

Week 9-10: Policy Deployment

- Finalize and approve policies through appropriate committees
- Conduct training for clinical staff and informatics teams
- Implement acceptable use controls
- Establish shadow AI detection

Week 11-12: Survey Readiness

- Compile Examiner Pack binders for Tier 1 systems
- Conduct mock survey/inspection
- Remediate gaps
- Establish ongoing monitoring cadence and board reporting

Chapter 14: Maturity Progression

Five Levels of Clinical AI Governance Maturity

Level	Name	What It Looks Like	Timeline
1	**Foundational**	Basic inventory exists, policies drafted but inconsistently applied	Current state
2	**Structured**	Complete inventory with tiering, policies approved, validation for Tier 1	6-12 months
3	**Managed**	Automated inventory, consistent validation, continuous monitoring, survey-ready	12-24 months
4	**Optimized**	Real-time performance visibility, automated compliance checking, predictive safety	24+ months
5	**Cryptographically Verifiable**	Every clinical AI decision produces evidence-grade artifact; mathematical proof of compliance	Platform investment

Level 5: The Evidence-Based Governance Frontier

At Level 5, clinical AI governance reaches its most mature state: every consequential AI action produces a verifiable record that answers "how do you know?" with mathematical certainty.

> **The Clinical Audit Artifact:** Level 5 systems produce cryptographic proof containing: immutable clinical decision record, algorithm version identifier, input/output data hashes, clinical policy alignment verification, clinician attestation, and replay instructions. This transforms clinical AI governance from assertion-based to evidence-based.

This is the logical endpoint of the authorization boundary principle: governance exists at the point where outputs become clinical decisions, and evidence—not explanations—must exist. Organizations pursuing Level 5 maturity should evaluate infrastructure vendors (including FERZ, which developed the frameworks in this guide) that provide cryptographically verifiable runtime governance, fail-closed execution architectures, and deterministic audit trails that meet FDA evidence standards.

 •

Appendix A: Clinical AI System Intake Form

Every clinical AI use case must submit this form before deployment.

Field	Description / Options
Use Case Name	[Free text - descriptive name]
Clinical Owner	[Name, title, department - single accountable clinician]
AI System/Tool	[Vendor/product name, or internally developed description]
Governance Track	☐ Decisioning AI ☐ Communications AI ☐ Both
Clinical Purpose	[What clinical problem does this solve? What decisions/outputs?]
Patient Population	[Who will this AI be used for?]
Output Type	☐ Diagnostic ☐ Treatment ☐ Prognostic ☐ Documentation ☐ Communication
Data Classes	☐ PHI ☐ De-identified ☐ Imaging ☐ Genomic ☐ Device data
Regulatory Status	☐ FDA cleared ☐ FDA exempt ☐ Under review ☐ Unknown
Automatic Tier 1 Trigger?	☐ Yes (specify which) ☐ No
Proposed Tier	☐ Tier 1 ☐ Tier 2 ☐ Tier 3 ☐ Tier 4
Tier Justification	[Brief explanation]

Appendix B: Tier 1 Clinical AI Control Checklist

All controls required before Tier 1 clinical AI go-live:

TIER 1: CRITICAL — All controls required before clinical go-live

- ☐ ☐ Designated clinical owner with documented accountability
- ☐ ☐ Intended use statement and patient population defined
- ☐ ☐ Automatic Tier 1 trigger assessment documented
- ☐ ☐ FDA regulatory status determined and documented
- ☐ ☐ Training data demographics and representativeness documented
- ☐ ☐ Clinical validation completed with performance metrics
- ☐ ☐ Demographic subgroup analysis completed
- ☐ ☐ Evidence-grade audit artifacts configured (not just logging)
- ☐ ☐ Clinician oversight mechanism implemented
- ☐ ☐ Clinical incident reporting path defined
- ☐ ☐ Vendor minimum evidence package collected (if third-party)
- ☐ ☐ HIPAA/privacy review completed
- ☐ ☐ Clinical AI Subcommittee / MEC approval documented
- ☐ ☐ Examiner Pack binder compiled
- ☐ ☐ Performance monitoring and review schedule established

Appendix C: Regulatory Reference Summary

Regulation/Guidance	Scope	Key Clinical AI Requirements
FDA SaMD Guidance	Medical device software	Risk classification, GMLP, clinical validation, post-market surveillance
21 CFR Part 820	Medical devices	Quality System Regulation, design controls, documentation
21 CFR Part 11	Electronic records	Audit trails, access controls, electronic signatures, data integrity
HIPAA	Covered entities	Privacy, security, minimum necessary, BAAs, breach notification
CMS CoP	Medicare providers	QAPI, medical staff, patient rights, information management
Joint Commission	Accredited orgs	Leadership, performance improvement, information management
EU AI Act	EU market access	High-risk classification for medical devices, conformity assessment

For questions on implementation or to discuss cryptographically verifiable governance infrastructure: ferz.ai

