IMPACT Healthcare Solutions

Future Proofing Your Organization with Smart AI Governance

Navigating the evolving AI law landscape and implementing effective governance in your organization

Landon Tooke, JD, MLS, CHC, CCEP, CHBME

IMPACT
Healthcare Solutions

Where AI Innovation Meets Compliance Intelligence.

Today's Roadmap

1. Why AI Governance Matters Now
2. Regulatory Landscape & Business Case
3. Understanding AI Governance Frameworks
4. The Compliance Connection: Integration Strategy
5. Operationalizing Governance in Healthcare
6. Real-World Scenarios & Implementation Pitfalls
7. Preparing for the Regulatory Future
8. Your First Steps Forward

AI Liability – The Reality

If you are not doing something like what I am talking about today, you are likely **negligent**.

AI Liability – A Licensing Regime, or Maybe Not?

1. Early AI policy discussions often focused on ex ante controls, including licensing-style oversight, registration, audits, and approval frameworks.
2. Those proposals have not become the dominant federal model.
3. The current environment remains fragmented, with deregulation rhetoric at the federal level and continued activity at the state level.
4. Congress is now also looking at product liability as a way to force safer AI design and deployment.

Enter The AI Lead Act

1. Would classify AI systems as "products" for liability purposes.
2. Would create a federal cause of action for harm caused by an AI system.
3. Claims could include **defective design**, **failure to warn**, **breach of express warranty**, and **unreasonably dangerous or defective product** theories.
4. Lawsuits could be brought by private parties, class plaintiffs, state attorneys general, and the U.S. Attorney General.
5. **Deployers** can also be treated as developers if they substantially modify or intentionally misuse an AI system.
6. Targets contractual provisions that unreasonably waive rights or limit liability.
7. Foreign AI developers would have to designate an agent for service of process before making AI systems available in the United States.

AI Is Here, Governance is Not

Before Governance

- ✗ Shadow AI use cases proliferating
- ✗ Inconsistent approval processes
- ✗ No unified risk framework
- ✗ Siloed decision-making
- ✗ Regulatory scrutiny increasing

AI Is Here, Governance is Not

With Governance

- ✓ AI adoption is *inevitable*
- ✓ Governance creates *efficiency*, not friction
- ✓ Smart governance = competitive advantage
- ✓ Organizations that govern well *move faster*
- ✓ Compliance is uniquely positioned to lead

The Regulatory Wake-up Call

DOJ Expectations on AI

Date	Development	Impact on Your Organization
Mar 2024	DAG Lisa Monaco: DOJ "laser-focused" on AI; enhanced penalties for AI-enabled crimes	Compliance officers must assess AI risks in compliance programs
Sep 2024	ECCP Guidance Updated	DOJ will evaluate how companies assess and manage AI risk
Jan 2025	Executive Order on AI	Federal agencies shift toward "pro-growth" AI policies
Apr 2025	OMB M-25-21 Memorandum	Minimum risk management practices for high-impact AI use cases

The Business Case for AI Governance

Four Compelling Reasons to Govern AI Now…

1) Data is the new oil

2) Shadow AI Costs You

3) Regulatory Environment is Fragmenting Fast

4) Governance Accelerates, Not Slows, Innovation

RCM Use Cases

Where AI Is Already Working

Use Case	What It Does	Key Governance Questions
Claims Prediction & Optimization	Predicts claim value, approval likelihood, optimal submission timing	Accuracy? Bias testing? Explainability to customers?
Fraud Detection	Flags unusual billing patterns, referral relationships, outlier behaviors	False positive rate? Human review? FCPA/anti-bribery checks?
Prior Authorization	AI recommends approve/deny based on historical patterns	Clinical safety? Provider appeal process? HIPAA compliance?
Patient Eligibility & Verification	Verifies coverage, identifies pre-authorization needs, predicts denials	Accuracy for vulnerable populations? Update frequency?
Revenue Cycle Analytics	Forecasts revenue, identifies bottlenecks, recommends process improvements	Data quality? Explanation to finance stakeholders?
Accounts Receivable Management	Prioritizes follow-up on high-value accounts, predicts collection likelihood	Fair debt collection practices? Bias across demographics?

Major AI Governance Frameworks

Player's Choice—Then Supplement

Framework	Origin	Best For	Key Strength
NIST AI Risk Management Framework	U.S. (NIST)	Most U.S. organizations; regulatory alignment	Risk-based, flexible; aligns with DOJ expectations
ISO/IEC 42001	International	Global operations; standards-driven organizations	Comprehensive; auditable; internationally recognized
EU AI Act Guidelines	European Union	International operations; healthcare tech vendors	Transparent, high-protection standard; driving global expectations
OMB M-25-21	U.S. Federal	Procurement, federal contractors, government collaboration	High-impact AI focus; federal alignment

IMPACT Healthcare Solutions

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

ISO International Organization for Standardization

You do not need to choose between frameworks. Most organizations **adopt one primary** framework and supplement with sector-specific guidance.

EU Artificial Intelligence Act

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES · OFFICE OF MANAGEMENT AND BUDGET

NIST AI Risk Management Framework

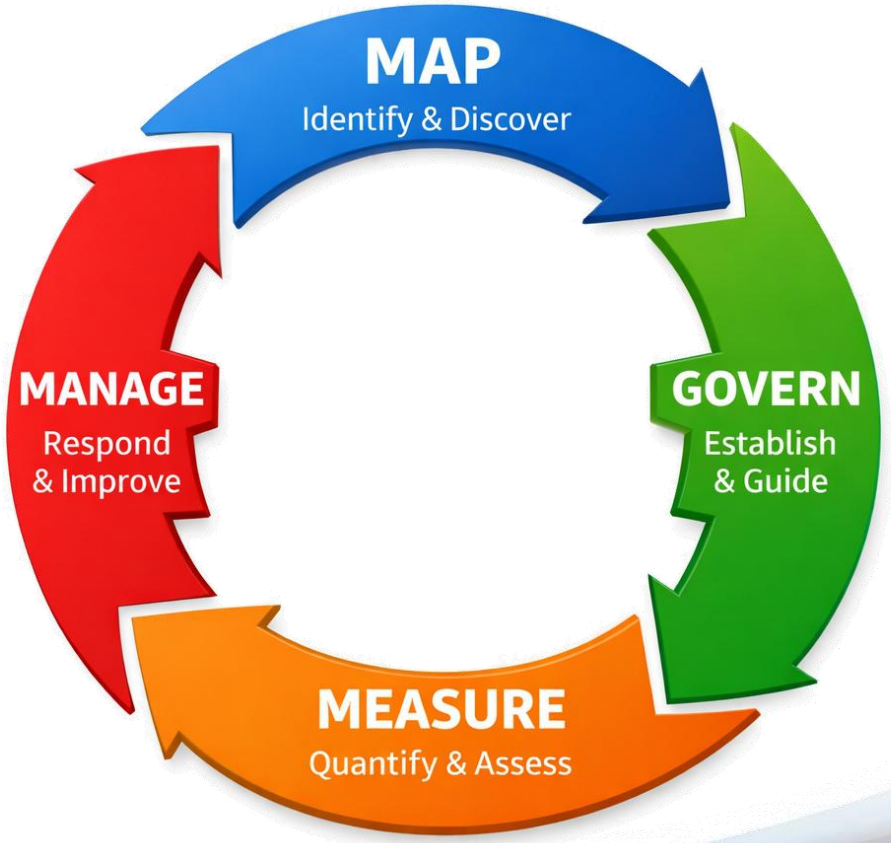
The Four Core Functions

MAP: What do we have? What could go wrong?

GOVERN: How do we govern it?

MEASURE: Are we performing?

MANAGE: What do we do when issues arise?



A Practical Translation for RCM

NIST Core Functions

Function	What It Means for You	Example
MAP	Inventory AI systems; identify risks (accuracy, bias, data quality, security)	*"We have 6 AI systems in RCM. This claims prediction model poses HIGH risk because it makes financial decisions affecting payment."*
GOVERN	Define governance structure, roles, policies, training	*"Compliance owns oversight. Data Science owns technical performance. Operations owns business logic. All escalate to AI Governance Committee."*
MEASURE	Set performance baselines; measure accuracy, bias, security, compliance	*"We test monthly for accuracy vs. human baseline. We test quarterly for bias across demographic groups. We log all decisions."*
MANAGE	Monitor performance; detect issues; respond quickly; improve controls	*"If accuracy drops below 95%, we escalate. If bias metrics drift, we retrain. If data breach occurs, we notify stakeholders within 24 hours."*

Why Compliance Leads AI Governance

Compliance is Uniquely Positioned to Lead AI Governance

Compliance Strength	Why It Matters for AI	Compliance Limitation
Balances risk, operations, and practicality	AI governance requires pragmatic risk decisions, not perfectionism	Not technical AI architects or data scientists
Understands documentation and defensibility	Regulators will ask "Why did the AI do that?" Compliance knows how to prepare answers	Not the system implementer or vendor
Neutral facilitator across functions	AI governance affects privacy, security, legal, IT, business—needs a bridge	Not the business owner or innovation leader
Builds governance programs that scale	Compliance programs already do: policy, training, auditing, escalation, monitoring	Not a one-time project; needs commitment
Manages related programs (privacy, security, ethics)	Foundation for AI governance already exists	Not the sole authority—needs cross-functional input

IMPACT
Healthcare Solutions

You are not starting from scratch.
You are adapting existing excellence to a new domain.

Does this mean that I must learn AI tech and data science?!?

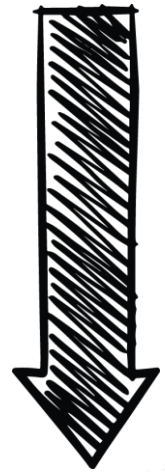
Governance Structure: A Layered Approach

Who Does What? (Sample governance structure)

Layer 1: AUTHORITY

Executive Sponsor (CEO/COO/CFO Level)

- Allocates resources
- Makes final decisions on strategic direction
- Escalation point for intractable issues



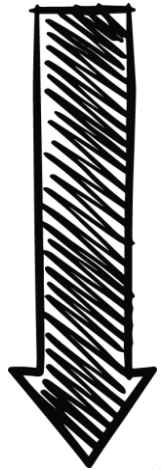
Layer 2: GOVERNANCE

AI Governance Committee (Cross-Functional)

Standing Members	Advisory Members
Compliance (Chair/Co-Chair)	RCM Leadership
Privacy Officer	Procurement
Security Officer	HR
Legal	Quality
IT/Data Science	Innovation/Strategy

Responsibilities

1. Define governance policies & standards
2. Review and approve AI use cases
3. Set risk appetite and classification
4. Approve escalations and exceptions
5. Monitor governance effectiveness



Layer 3: EXECUTION

Operational Working Groups

- Business units: AI use case owners
- Technical teams: implementation
- Compliance: ongoing oversight & monitoring
- Audit: periodic testing & validation

Step 1: Assess Your Current State

What to Inventory:

1. Transparent AI Use
   - Openly deployed AI systems (RCM platforms, commercial tools with AI)
   - Business case, use case, owner, data sources, current controls
2. Shadow AI Use
   - ChatGPT, Claude, or other tools employees are already using
   - Track frequency, use cases, data sources (What's being fed into these tools?)
   - Note: Not trying to eliminate shadow AI, but to see and manage it
3. Planned AI Initiatives
   - What's in development or planned for next 12-24 months?
   - Where is innovation heading?

Step 1: Assess Your Current State

Example Risk Assessment Profile

4. Risk Assessment of Current Use
    - Data sensitivity: Does the AI touch PHI? PII? Confidential business data?
    - Decision impact: Does AI make financial decisions? Clinical decisions? Payment decisions?
    - Regulatory exposure: Is this in a regulated domain (healthcare, employment, lending)?
    - Risk classification: HIGH (high sensitivity + high impact), MEDIUM, LOW

Step 1: Assess Your Current State

Example Inventory:

AI System	Current Status	Data Sensitivity	Decision Impact	Regulatory Domain	Risk Level	Owner	Current Controls
ChatGPT	Shadow/ Widespread	Potentially HIGH depending on use	LOW (research/ drafting)	Privacy/ Compliance	MEDIUM	TBD	No Formal Controls
Claims Prediction Model	In Production	PHI	HIGH (payment decisions)	Healthcare/ Finance	HIGH	Rev Cycle VP	Manual override on high-value claims

Step 2: Establish Intake & Decision Workflow

AI Initiative Submitted

1. TRIAGE

- Quick risk assessment
- Low-risk? FAST TRACK
- High-risk? FULL REVIEW
- Duration: 1 Week

2. FULL ASSESSMENT

- Evaluate against framework
- Assess data, decisions, risks
- Subject matter input (privacy,
- Security, legal, etc.)
- Duration: 2 Weeks

3. COMMITTEE DECISION

- Present assessment
- Vote: approve, approve w/cond.
- defer, reject
- Document decision rationale
- Duration: Committee Meeting

✓ Approved

✓ Approved w/Cond. - *What are they?*

✗ Deferred - *Plan to reconsider?*

✗ Rejected

Step 2: Establish Intake & Decision Workflow

Intake Intelligence Over Time

- Intake data tells a story about how your organization uses AI
- Patterns reveal governance gaps and priorities
- Informs policy updates, training focus, emerging risks
- Demonstrates organizational maturity to regulators

Step 3: Formalize Expectations with Policies & Standards

Step 3: Formalize Expectations with Policies & Standards

Core Policies & Standards to Develop:

1. **AI Use Policy –** tells people where AI is allowed, where it is not, who is responsible, and when the rules must be updated.
2. **Data Quality & Testing Standards –** make sure AI uses accurate data, is tested regularly, and has written records of results and fixes.
3. **Bias & Fairness Standards –** help the organization find unfair results, set fairness targets, test on a schedule, and act quickly when problems appear.
4. **Explainability & Transparency Standards –** require that AI decisions can be understood, are documented, and are clearly explained to users and, when needed, to customers or patients.
5. **Privacy & Security Standards –** protect data used by AI, control what can be shared with outside tools, and align AI use with breach rules and HIPAA.

Step 3: Formalize Expectations with Policies & Standards

Step 3: Formalize Expectations with Policies & Standards

Core Policies & Standards to Develop:

1. **Data Privacy –** Prevents sensitive data leaks into models and prompts.
2. **Access Control –** Stops unauthorized employees from using AI systems improperly.
3. **Model Usage –** Avoids teams using random models without approval.
4. **Prompt Handling –** Prompts can expose secrets and private customer details.
5. **Data Retention –** Keeps you compliant and reduces long-term risk exposure.
6. **AI Security –** AI systems are vulnerable to prompt injection & jailbreaks.
7. **Human-in-the-Loop –** Prevents AI from making irreversible bad decisions.
8. **Explainability –** Enterprises must justify AI decisions, especially in regulated domains.

Step 3: Formalize Expectations with Policies & Standards

Core Policies & Standards to Develop:

9. **Audit Logging –** Without logs, you cannot debug failures or prove compliance.
10. **Bias & Fairness –** Biased models can harm customers and trigger legal risk.
11. **Model Evaluation –** Prevents "looks good" models from failing in production.
12. **Monitoring & Drift –** AI performance degrades silently over time.
13. **Vendor Governance –** External AI providers can introduce hidden compliance risks.
14. **IP Protection –** AI usage can leak company IP and internal knowledge.
15. **Incident Response –** AI failures need fact containment like any production outage.
16. **Responsible AI –** Ensures AI is used ethically, safely, and transparently.

Step 4: Training & Communication

Who needs training? (Sample training schedule)

Audience	Focus	Format	Frequency
Executive Leadership	Governance structure, risk posture, oversight responsibilities, business case	Executive briefing (30-45 min)	Annually + as policies change
Compliance/Risk Team	Deep governance framework, intake process, audit procedures, escalation	In-depth training (2-4 hours)	At program launch; quarterly updates
AI Governance Committee	Each function's role, decision framework, policy rationale, case studies	Committee orientation (2 hours)	Quarterly + ad-hoc as needed
Business Unit Leaders	How to submit AI initiatives, policy expectations, approval process	Dept. briefing (30-60 min)	Quarterly
End Users	Responsible AI use, limitations, escalation, acceptable uses	Online module + posters	Onboarding + annually
Technical Teams	Data quality standards, testing protocols, documentation, compliance integration	Technical workshop (2 hours)	At program launch; annual refresh

Step 4: Training & Communication

Key Training Content for **Everyone**

1. **Why does AI governance exist?** Business case, regulatory expectations, organizational benefits
2. **How does the Intake Process work?** What triggers review, who decides, how fast decisions happen?
3. **What do we expect?** Data quality, testing, bias monitoring, human oversight, documentation
4. **What happens if things go wrong?** Escalation, incident response, remediation expectations
5. **Can I have examples?** Real examples (anonymized) of approved, deferred, and rejected initiatives—and why.

Step 5: Monitoring & Oversight

The Three Pillars of Oversight

Operational Monitoring—Does the AI work?

1. Question: Is the AI system performing as intended?
2. Frequency: Continuous (automated alerts) or monthly
3. What to measure:
   - Accuracy vs. baseline human performance
   - Performance consistency—is it stable or drifting?
   - Bias—are disparities emerging across demographics?
   - Data quality—is the input data still clean?
4. Who: Data Science team + Compliance spot-checks
5. Action: If performance drops >5%, escalate

Step 5: Monitoring & Oversight

The Three Pillars of Oversight

Compliance Monitoring—Are my team members following policies?

1. Question: Is the AI system being used as approved? Are controls effective?
2. Frequency: Quarterly
3. What to audit:
   - Usage logs—is it being used for approved purposes only?
   - Decision logs—are decisions documented?
   - Human override rate—is human review happening as required?
   - Data handling—is PHI protected? Is data deletion happening on schedule?
   - Policy adherence—is training completed? Escalations working?
4. Who: Compliance + Audit
5. Action: Report findings to governance committee; corrective action if issues found

Step 5: Monitoring & Oversight

The Three Pillars of Oversight

Governance Oversight—Are we making smart decisions?

1. Question: Are governance structures working? Do we need to adapt?
2. Frequency: Quarterly committee meeting
3. What to review:
   - Intake trends—how many applications? Risk distribution? Approvals vs. rejections?
   - Performance trends—which AI systems are working well? Which are struggling?
   - Emerging risks—new use cases appearing? New regulations? New concerns?
   - Program maturity—are we getting better? Faster? More consistent?
4. Who: AI Governance Committee
5. Action: Approve policy adjustments, resource allocation, strategic priorities

Audit & Documentation – The "Why"

Why Documentation Matters:

"Why did your AI system do that?"

"How do you know it's fair?"

"How do you know it's working?"

You must answer with evidence, not feelings.

Your Best Defense

Documentation shows you had governance, you tested, you monitored, and you acted when problems arose.

Audit & Documentation – The "Why"

Key Documentation Principles

1. **Be Specific:** Document date, person, action taken, and outcome.
2. **Be Contemporaneous:** Document when you did it, not after the fact.
3. **Be Defensible:** Show your reasoning, alternatives considered, and your decision rationale.
4. **Be Consistent:** Use the same documentation template and format across all AI systems.

Audit & Documentation – The "Why"

Sample Audit Checklist for AI Systems

- ❑ Development decision documented with governance approval
- ❑ Pre-deployment testing completed and documented (accuracy, bias, security)
- ❑ Performance baseline established and documented
- ❑ Monthly/quarterly monitoring completed (results documented)
- ❑ Incidents escalated and resolved (incident log maintained)
- ❑ Users trained on system capabilities and limitations
- ❑ Privacy impact assessment completed
- ❑ Security assessment completed
- ❑ Compliance assessment completed
- ❑ Decision logs maintained (what did AI recommend? What did human decide?)

Putting It All Together

Real-World Scenarios

Scenario 1—Deploying a Claims Prediction Model

Playing with the shiny new toys…

Situation: Your revenue cycle team wants to deploy an AI model that predicts claim approval likelihood and recommends optimal submission timing. You expect to save $1MM annually in operational costs.

Scenario 1—Deploying a Claims Prediction Model

Governance Flow:

1. INTAKE
   - Revenue Cycle VP submits proposal
   - Initial assessment: HIGH RISK (makes financial decisions, touches claim data)
   - Triggers full review (HIGH-risk fast-track)

2. FULL ASSESSMENT
   - Data Privacy: PHI involved—needs HIPAA security review
   - Data Science: Accuracy tested at 97% vs. 89% human baseline ✓
   - Bias Testing: Checked across 5 demographic groups—all within 3% parity ✓
   - Operations: No negative impact, financial impact approved by CFO ✓
   - Security: Data access controls, breach notification, audit trail ✓
   - Legal: No contractual issues with vendors/payers ✓

Scenario 1—Deploying a Claims Prediction Model

Governance Flow:

3. COMMITTEE DECISION
   - Decision: APPROVED WITH CONDITIONS
   - Conditions:
     - Monthly accuracy monitoring—alert if drops below 95%
     - Quarterly bias testing—alert if disparity >5%
     - Human override required for claims >$10k
     - 90-day pilot with high-volume facility before rollout
     - Monthly governance committee updates during pilot

4. IMPLEMENTATION
   - System deployed in pilot facility
   - Decisions logged in system (AI recommendation + human decision)
   - Monthly reports to governance committee

Scenario 1—Deploying a Claims Prediction Model

Governance Flow:

5. MONITORING (MONTH 1-3)
   ✓ Accuracy: 96.8% - 97.2% (stable) → No action
   ✓ Human override rate: 8% (acceptable) → No action
   ✓ Bias testing: <2% disparity → No action
   → PILOT APPROVED FOR ROLLOUT

6. ONGOING (POST-ROLLOUT)
   - Monthly accuracy monitoring continues
   - Quarterly bias testing continues
   - Annual policy review to assess if conditions still appropriate
   - Incident escalation if problems detected

Scenario 2—Shadow AI Response

The ChatGPT nightmare…

Situation: During shadow AI inventory, you discover that a claims processor has been pasting actual claims data—including names, dates of birth, claim numbers, and clinical details—into ChatGPT asking it to identify denial reasons, suggestions on corrections and documentation, and to draft appeal letters.

Scenario 2—Shadow AI Response

Governance Response:

1. ASSESS THE RISK—ESCALATION ALERT!
   - Data Sensitivity: PHI → CRITICAL RISK
   - Data Destination: OpenAI servers (third-party, not HIPAA-covered entity) → CRITICAL RISK
   - Decision Impact: decisions about claims based on ChatGPT responses → HIGH RISK
   - Regulatory Exposure: HIPAA violation potential; possible data breach; CMS compliance issue → CRITICAL RISK
   - Overall Risk: CRITICAL/HIGH ❌

2. IMMEDIATE RESPONSE
   - Notify employee of compliance concern
   - Instruct employee to STOP behavior immediately
   - Initiate compliance program's security breach protocol

5 Common Pitfalls

1. Analysis Paralysis

- Why it happens: You wait for the perfect framework or perfect conditions to begin.
- How to prevent it: Start with structure, not perfection. Choose one framework. Do it 80% right rather than waiting for 100%.
- How to fix it: Pick NIST, start with assessment, begin intake immediately. Perfection evolves.

2. Siloed Governance

- Why it happens: Compliance "owns" it; business ignores it for failure to see value.
- How to prevent it: Make it collaborative from day one. Position governance as enabling innovation, not blocking it. Show business the benefits.
- How to fix it: Educate business units on benefits. Celebrate approvals as much as you oversee. Invite business leaders to committee.

5 Common Pitfalls

3. Innovation Slow-Down

- Why it happens: Every AI idea takes 6 months to approve; business loses interest.
- How to prevent it: Use risk-based approach. Low-risk ideas get expedited. High-risk ideas get full review. Medium-risk gets middle ground.
- How to fix it: Re-evaluate your triage process. Are you being too conservative? Talk to business leaders about approval timeline targets. Adjust.

4. Overwhelming Scope

- Why it happens: You try to govern everything at once; program becomes abureaucratic nightmare.
- How to prevent it: Use a phased approach: Phase 1—Establish structure, assess existing use, start intake. Phase 2—Develop policies, train committee. Phase 3—Full monitoring, continuous improvement.
- How to fix it: Pause and re-prioritize. Start with HIGH-risk systems only. Expand scope as you mature.

5 Common Pitfalls

5. Loss of Momentum

- Why it happens: Program launches, then fades. Committee meetings become irregular. People do not know status.
- How to prevent it: Establish regular meeting cadence. Use intake and monitoring findings to drive agendas. Celebrate wins publicly.
- How to fix it: Emergency restart. Get executive sponsor to re-commit. Reschedule meetings. Communicate status quarterly to board/leadership. Show progress.

Measuring Governance Maturity—Where Are You Today?

Level 1: Informal—Current state for most

- No formal AI governance structure
- Decisions about AI are made without consistent framework
- Documentation is sparse or informal
- Limited cross-functional input

Level 2: Defined—Months 1-3

- Governance committee established
- Intake process exists (even if basic)
- Policies are drafted or in development
- Some documentation of decisions

Measuring Governance Maturity—Where Are You Today?

Level 3: Integrated—Months 3-6

- Intake is documented and consistent
- Policies are approved and communicated
- Monitoring is systematic (dashboards, regular reporting)
- Integration with compliance is clear

Level 4: Proactive—Months 6-12+

- Risk-based triage allows fast approvals for low-risk items
- High-risk items get appropriate scrutiny
- Proactive monitoring detects trends and emerging risks
- Organization is ahead of regulatory changes

Measuring Governance Maturity—Where Are You Today?

Level 5: Strategic—Months 12+

- Governance is embedded in culture
- Innovation and compliance are balanced
- Organization is an industry thought leader
- Regulatory partnerships exist

Sample Action Plan—Your First 30 days

Week 1: Foundation

- Secure executive sponsor
- Identify AI Governance Committee lead
- Do a quick shadow AI inventory

Week 2: Structure

- Schedule first committee meeting
- Select your framework
- Draft committee charter

Action Plan—Your First 30 days

Week 3: Process

- Design intake process
- Define initial policies
- Plan communications

Week 4: Launch

- Hold first committee meeting
- Launch communications
- Begin intake review
- Schedule policy training

Future-Proofing Is Your Competitive Advantage

Three Truths about AI Governance

Truth 1: Governance Does Not Stop Innovation—It Enables It

- Organizations with mature governance move faster, not slower
- Clear framework = faster decisions
- Low-risk ideas get expedited approvals
- Business moves with confidence, not surprises

Future-Proofing Is Your Competitive Advantage

Three Truths about AI Governance

Truth 2: You Do Not Have to Be Perfect to Start

- Governance matures over time (Level 1 → Level 5)
- Start with structure, let it evolve
- Better 80% governance than 0% governance while you wait for perfect
- Every organization starts where you are
- This is your moment to be a strategic leader, not just a risk manager

Future-Proofing Is Your Competitive Advantage

Three Truths about AI Governance

Truth 3: Compliance Is Uniquely Positioned to Lead

- You already have governance infrastructure (policy, training, auditing, escalation)
- You already balance risk and operations
- You already speak the languages of Legal, Privacy, Security, and Business
- This is your moment to be a strategic leader, not just a risk manager

IMPACT
Healthcare Solutions

AI governance is not about saying "no" to innovation. It is about creating a framework that lets your organization say "YES" with confidence—confidence that you are complying with regulations, managing risks, and positioning yourself to lead in this new era of healthcare technology.

Questions?

IMPACT Healthcare Solutions

TOOKE LAW

Landon Tooke

ltooke@impact-healthcare.net

landon@tookelaw.com

318-955-9730