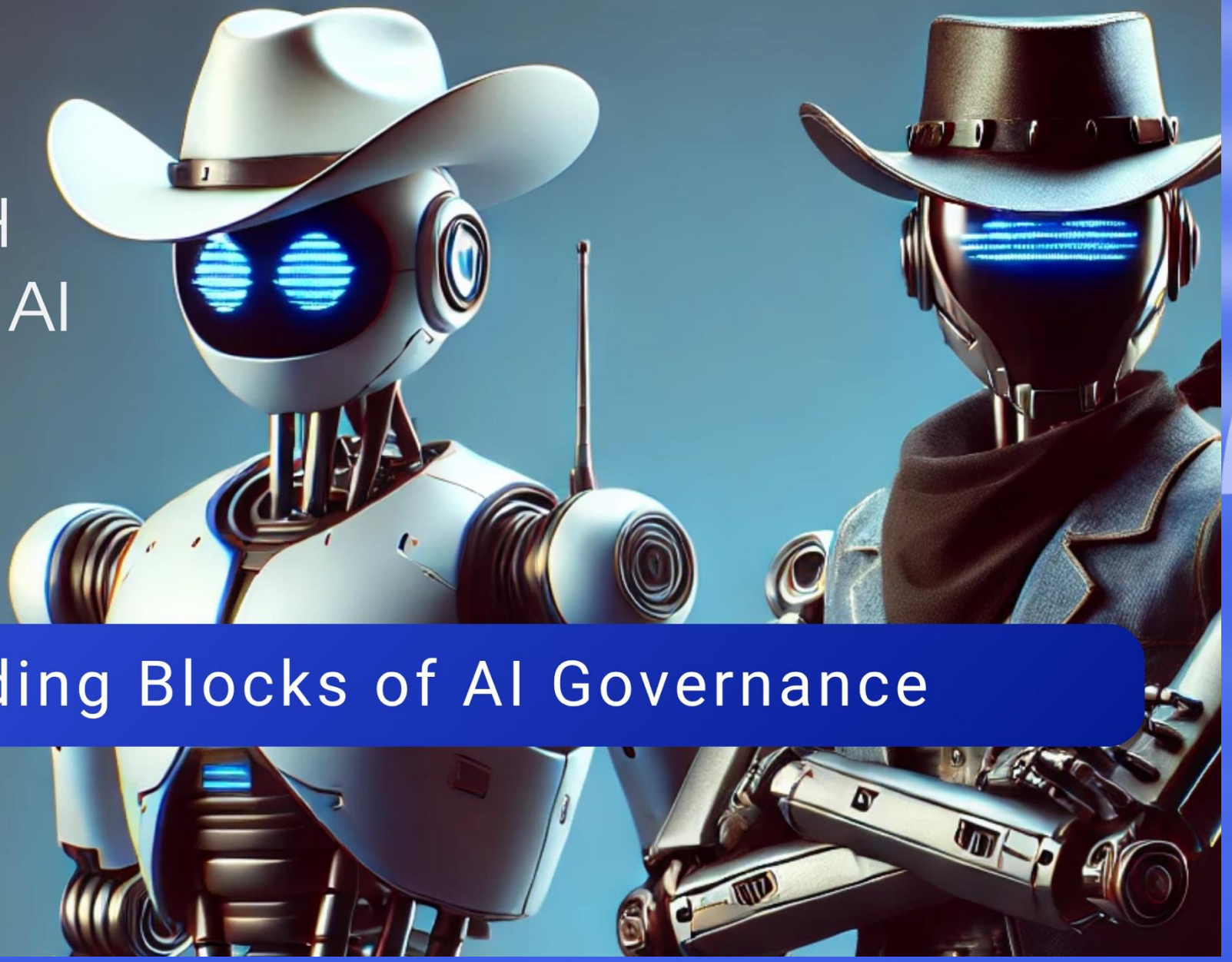
LEADING WITH RESPONSIBLE AI

Day 1: Laying the Foundations for Responsible AI



The Building Blocks of AI Governance

Clearwater

Meeting Logistics

Microphones

All attendees are on mute.

Questions

Type your questions in the Q&A box.

Resources

Upcoming events, slides & resources linked.

Recording

Recording will be provided after event.

Survey

Survey will prompt at the end of webinar.

Agenda

- Welcome + Introductions
- Presentation Content: The Building Blocks of AI Governance
- Q+A

Jon Moore, MS, JD, CHISL, HCISPP

Chief Risk Officer and Senior Vice President of Consulting Services

Clearwater

The Building Blocks of AI Governance

Jon Moore, MS, JD, HCISPP

Chief Risk Officer & SVP Consulting Services, Clearwater

Clearwater

An Executive Imperative

AI is embedded in healthcare delivery—from diagnostic tools to operations. Executive-level governance is needed now to prevent risk and realize value.

AI Application	Description	Supports Delivery/Operations
Diagnostic Imaging	ML analyzes images for accurate detection.	Delivery: Improves precision, speeds care.
Predictive Triage	AI predicts patient risks using EHR data.	Delivery: Prioritizes cases, optimizes resources.
NLP for Notes	NLP automates clinical note documentation, coding.	Operations: Reduces admin, boosts accuracy.
RPA for Supply Chain	AI automates inventory, procurement processes.	Operations: Ensures supplies, cuts costs.
Virtual Assistants	AI chatbots support patients, scheduling, reminders.	Delivery: Enhances engagement, treatment adherence.
Surgical Robots	AI enhances robotic surgery with precision, analytics.	Delivery: Boosts accuracy, reduces recovery time.

What Happens without Governance

Without governance, AI failures lead to patient harm, compliance breaches, and reputational damage.

Category	Example	Description and Impact
Patient Harm	Epic Sepsis Prediction Model (2021-2025)	Epic's AI model for predicting sepsis in hospitals identified only 33% of sepsis cases, raising false alarms and missing critical patients, potentially delaying life-saving treatment. Impact: Increased risk of patient mortality and prolonged hospital stays due to inaccurate predictions.
Patient Harm	2019 Healthcare Algorithm Bias	A widely used US algorithm for high-risk care management underestimated risk for Black patients by using healthcare spending as a proxy, leading to reduced access to critical care programs. Impact: Exacerbated health disparities, with sicker Black patients receiving less care.
Compliance Breaches	Agentic AI/Serviceaide – Catholic Health System Breach (2025)	In May 2025, a significant data breach occurred involving Agentic AI, a company specializing in autonomous AI systems for healthcare. The breach exposed the personal and protected health information (PHI) of 483,126 patients from Catholic Health in Buffalo, New York. Impact: likely class-action lawsuit/s and OCR investigation.
Reputational Damage	IBM Watson for Oncology (2013-2017)	IBM Watson's oncology tool, partnered with MD Anderson, failed to meet clinical goals, leading to project termination and public criticism. Impact: Loss of trust from healthcare providers and patients, damaging IBM's reputation in healthcare AI.

AI Governance vs Strategy

Governance ensures AI is safe and compliant; strategy ensures it creates value. Both are essential and must work together.

AI Strategy

A roadmap for adopting and scaling AI to achieve organizational goals, such as improving patient outcomes, operational efficiency, or innovation. It focuses on what AI will do and how it aligns with healthcare priorities.

Key focus:

- identifying AI use cases (e.g., diagnostics, predictive analytics).
- Aligning AI with clinical and operational needs.
- Driving innovation and competitive advantage.

AI Governance

A framework of policies, processes, and controls to ensure AI is developed, deployed, and monitored responsibly. It focuses on how AI is managed to ensure ethics, compliance, and safety.

Key focus:

- Ensuring compliance with regulations (e.g., HIPAA, GDPR).
- Mitigating risks (e.g., bias, errors, breaches).
- Promoting transparency, accountability, and trust.

Leadership’s Role in Governance

Executives must define AI governance mandates, maintain inventory, assign cross-functional accountability, and align initiatives with risk tolerance.

Responsibility	Definition	Healthcare Context
Define AI Governance Mandates	Set policies and standards for AI use.	Rules for bias audits, HIPAA compliance.
Maintain AI Inventory	Record all AI systems, purpose, status.	Tracks triage, NLP tools for oversight.
Assign Cross-Functional Accountability	Designate roles across departments for AI oversight.	Clinicians, IT, legal collaborate to reduce risks.
Align Initiatives with Risk Tolerance	Match AI projects to risk capacity.	Prioritize low-risk scheduling over high-risk diagnostics.

The Four Pillars of AI Governance

The ethical and operational foundation of AI oversight.

Safety

Ensuring AI systems minimize harm to patients by delivering accurate, reliable, and unbiased outcomes. Safety involves rigorous testing, validation, and monitoring of AI models to prevent errors or adverse effects.

Accountability

Establishing clear roles and responsibilities for AI development, deployment, and oversight. Accountability ensures individuals or teams are answerable for AI performance and ethical use.

Compliance

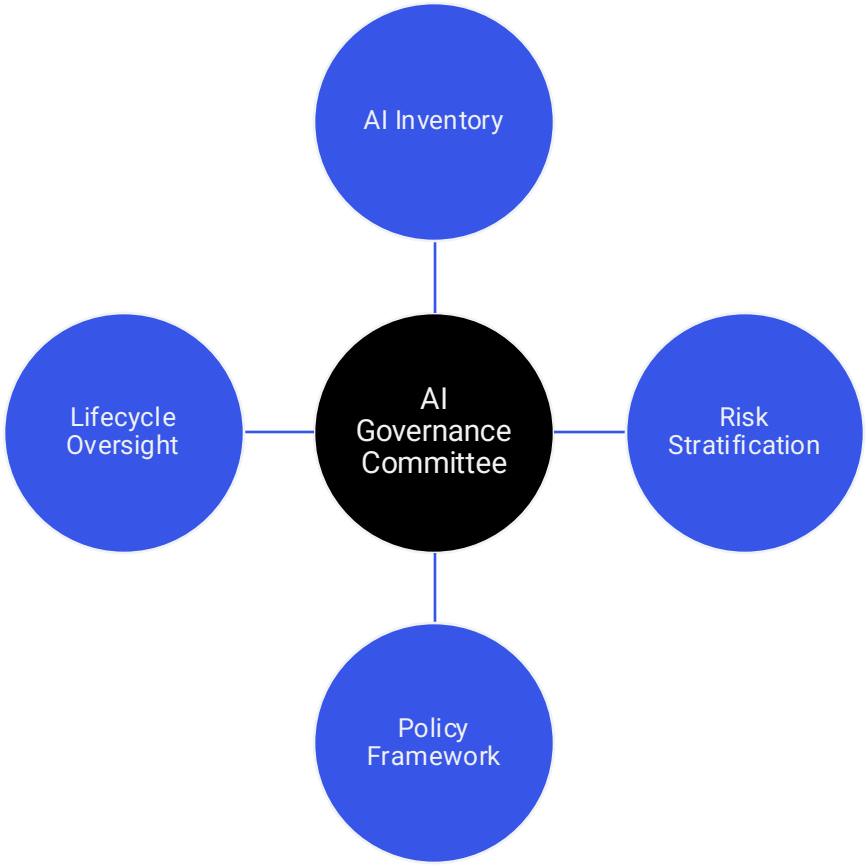
Adhering to legal, regulatory, and ethical standards governing AI, such as HIPAA, GDPR, and FDA requirements. Compliance involves aligning AI practices with data privacy, clinical, and operational regulations.

Transparency

Providing clear, understandable information about AI systems, including their purpose, data sources, decision-making processes, and limitations. Transparency fosters trust and enables informed use.

What Governance Looks Like in Practice

Governance is continuous and embedded.



AI Committee: Ensures collaborative decision-making, aligning AI with patient safety and organizational goals.

AI Inventory: Enables oversight, supports audits, and prevents untracked AI risks (e.g., outdated models).

Risk Stratification: Aligns AI initiatives with risk tolerance, minimizing patient and organizational harm and compliance breaches.

Policy Framework: Provides consistency, ensures compliance, and reduces legal and ethical risks.

Lifecycle Oversight: Maintains AI reliability, prevents degradation, and ensures accountability throughout use.

Governance Frameworks You Can Use

Adaptable frameworks help structure AI governance.

Organization	Framework	Description	Relevance to Healthcare
NIST	NIST AI Risk Management Framework (RMF)	Voluntary framework to assess and mitigate AI risks via governance and measurement.	Standard for AI management, covering governance, risk, compliance.
	Singapore's Model AI Governance Framework	Promotes human-in-the-loop, transparent, adaptive governance for trust.	Ensures clinicians validate AI outputs (e.g., triage tools), fostering trust and GDPR compliance.
IEEE Computational Intelligence Society	OECD/IEEE AI Principles	Ethical AI principles focusing on inclusivity, transparency, accountability.	Mitigates biases (e.g., 2019 algorithm disparities), ensuring equitable care and public trust.
	EU AI Act	Regulates high-risk AI, mandating safety, transparency, compliance.	Ensures safe diagnostics, avoids EU fines.
ISO 42001	ISO/IEC 42001 AI Management System Standard	Standard for AI management, covering governance, risk, compliance.	Standardizes AI processes, enables auditability.
	WHO's Ethics and Governance of AI for Health	Standard for AI management, covering governance, risk, compliance.	Promotes equitable AI aligning with clinical ethics and global health goals.

Understanding the Risk Spectrum

Risks vary by context calling for stratified governance based on potential for patient harm or bias, organizational harm, and business disruption.

Operational AI: Administrative Automation. e.g., AI for billing or appointment reminders

Clinical AI: Predictive Analytics e.g., AI for patient triage or readmission risk

Clinical AI: Diagnostic Tools e.g., AI for cancer detection in imaging

Operational AI: AI-Powered Patient Chatbots handle routine patient inquiries

Operational AI: Resource Allocation e.g., AI for hospital bed or staff scheduling

Clinical AI: Treatment Planning e.g., AI-guided surgical robots

Clearwater

AI Inside and Outside Your Walls

Internally built AI needs end-to-end control. Third-party tools require robust vetting, contract language, and shared responsibility models.

Governance Responsibilities by AI Solution Type

Category	Internal	Third-Party	Hybrid
Model Control	●	○	◑
Training Data Ownership	●	○	◑
Explainability	●	◑	◑
Bias Testing	●	◑	◑
Compliance Responsibility	●	◑	◑
Monitoring and Updates	●	○	◑
Legal Exposure	●	◑	◑

Regulatory Horizon

Regulations are evolving. Governance ensures readiness.

Regulatory Source	Focus	Requirements	Governance
HIPAA (US)	Patient data privacy	Encrypt data, limit disclosures, notify breaches	Secure data, audit privacy, train staff
FDA (US)	Clinical AI as medical devices	Validate accuracy, monitor post-market	Validate AI, maintain FDA records
FTC (US)	AI advertising, consumer protection	Avoid deceptive claims, ensure transparency	Review marketing, disclose AI limits
Section 1557 (US)	Anti-discrimination, AI bias	Ensure fairness, audit for bias	Check bias, train on equity
EU AI Act (Global)	High-risk AI safety, transparency	Assess risks, ensure oversight, report incidents	Adopt risk frameworks, prepare audits
GDPR (Global)	Data protection, patient rights	Obtain consent, anonymize data	Use compliant data pipelines, conduct DPIAs

Operationalizing Governance

AI risks must live inside your broader risk and compliance systems.

Component	Integration with ERM	Healthcare Action
Incident Response	Extends ERM protocols to handle AI failures (e.g., misdiagnoses, data breaches).	Develop AI-specific response plans, train teams, report incidents per FDA/EU AI Act.
Audit	Incorporates AI risk assessments into regular ERM audits for performance, bias.	Conduct quarterly AI audits, check for bias (e.g., 2019 algorithm issues), use NIST RMF.
Procurement	Aligns AI vendor selection with ERM risk criteria (e.g., security, reliability).	Vet AI vendors for HIPAA/GDPR compliance, ensure transparency in contracts.
Compliance Tracking	Embeds AI regulatory compliance (e.g., HIPAA, FDA) into ERM monitoring systems.	Track AI compliance via dashboards, align with Section 1557, EU AI Act standards.
Risk Management	Evaluate risk on an ongoing basis and treat risks above organizational threshold	Conduct risk analysis on AI-enabled information assets inclusive of unique threats and vulnerabilities of AI solutions.

Implementing Controls and Guiderails

Implement controls that reduce risk to your organization's threshold.

Program Level Controls

Focus on organization-wide governance mechanisms (e.g., policies, oversight committees) that set the foundation for risk management across all AI initiatives.

Examples:

- AI Ethics Policy with bias audits
- Cross-functional AI oversight committee

System Level Controls

Highlight controls specific to individual AI systems (e.g., validation, monitoring) to mitigate risks in clinical or operational use.

Examples:

- Validation testing for diagnostic AI
- Real-time monitoring of triage AI

Continuous Monitoring & Maturity

Track: model accuracy, bias emergence, drift, incident frequency. Use a maturity model to guide continuous improvement and scaling.

Level	Characteristics	Healthcare Impact	Example Metrics
1. Reactive	• No governance or inventory • Risks unmanaged	High risk of errors (e.g., misdiagnoses), non-compliance.	• % AI tools inventoried • Policy adoption rate • Staff training completion rate • Regulatory violation incidents
2. Foundational	• Maintains AI inventory • Forms governance committee	Tracks tools, reduces oversight gaps, initial risk control.	
3. Integrated	• Embeds AI in procurement, IT • Aligns with ERM	Ensures compliance, mitigates bias (e.g., 2019 algorithm issues).	• Audit completion rate • Bias incidents detected
4. Optimized	• Monitors AI performance, drift • Formal incident response	Enhances safety, supports FDA/EU AI Act compliance.	• Model drift detection rate • Risk prediction accuracy • AI incident response time • Ethical compliance score
5. Proactive	• Predicts risks, tracks metrics • Integrates ethics, innovation	Prevents failures, aligns with NIST RMF, builds trust.	

Governance in Action: Real-World Examples

Governance enabled scale and safety—not just compliance.

KAISER PERMANENTE®

Demonstrates operational AI governance (transcription), with strong data privacy (HIPAA) and human oversight. Saves 3hrs/week for doctors, improves EHR Accuracy.

https://www.cbs8.com/article/news/local/kaiser-permanente-using-artificial-intelligence-to-improve-patient-care/509-4c4fef1a-4358-4c06-a224-35974ea0f6b3#:~:text=SAN%20DIEGO%20%E2%80%94%20Kaiser%20Permanente%20has,from%20documentation%20to%20patient%20care.

TEMPUS

Shows advanced governance for high-risk clinical AI (oncology), managing massive datasets ethically. Personalizes cancer treatments, matches clinical trials.

https://cancercommons.org/latest-insights/power-of-precision-medicine/

PHILIPS

Philips recognizes the need for centralized AI governance to ensure patient safety and data integrity, particularly within clinical documentation and revenue cycles.

https://www.philips.com/a-w/about/news/archive/standard/news/articles/2025/philips-chief-innovation-officer-shez-partovi-comments-on-navigating-the-eu-ai-act.html

Quick Wins: Your First 90 Days

Create your 30-60-90-day plan.

Phase	Actions	Outcomes
30 Days: Foundation	- Form AI governance committee - Build AI tool inventory - Engage stakeholders	Committee active, 100% tools inventoried, buy-in secured.
60 Days: Risk & Controls	- Classify AI risks (e.g., bias) - Define initial controls - Track basic metrics	Risks identified, controls implemented, metrics baseline set.
90 Days: Formalization	- Formalize AI policies - Establish oversight protocols - Train staff on governance	Policies enforced, oversight active, staff compliance ensured.

Final Thought

AI can expand equity, access, and outcomes. It can increase efficiency and effectiveness. Or it can amplify harm. **Governance is the steering wheel**. Leadership determines the destination.

Q&A

Today's Agenda – Coming Next

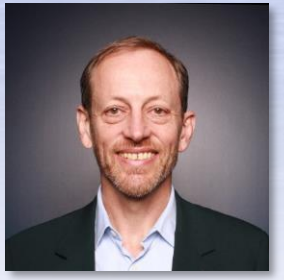
June 23

12:00 pm – 12:45 pm CT
Developing an AI Governance Program

Dave Bailey, VP Consulting Services, Security, Clearwater
Robin Lang, CIO, CaroMont Health


1:00 pm – 1:45 pm CT
Operationalizing AI Governance

Jon Moore, Chief Risk Officer & SVP Consulting Services, Clearwater
James Green, Chief Executive Officer, Cognome

Clearwater

We are here to help.

Moving healthcare organizations to a more secure, compliant, and resilient state so they can achieve their mission.

Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | linkedin.com/company/clearwater-security-llc/

Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.