LEADING WITH RESPONSIBLE AI

Day 1: Laying the Foundations for Responsible AI

Operationalizing 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 Toward the end of webinar.

Clearwater

Agenda

- Welcome + Introductions
- Presentation Content: Operationalizing AI Governance
- Q+A

Jon Moore, MS, JD, CHISL, HCISPP

Chief Risk Officer & SVP
Consulting Services
Clearwater

James Green

Chief Executive Officer
Cognome

Clearwater

Operationalizing AI Governance

Jon Moore, CRO & SVP Consulting Services, Clearwater
James Green, CEO, Cognome

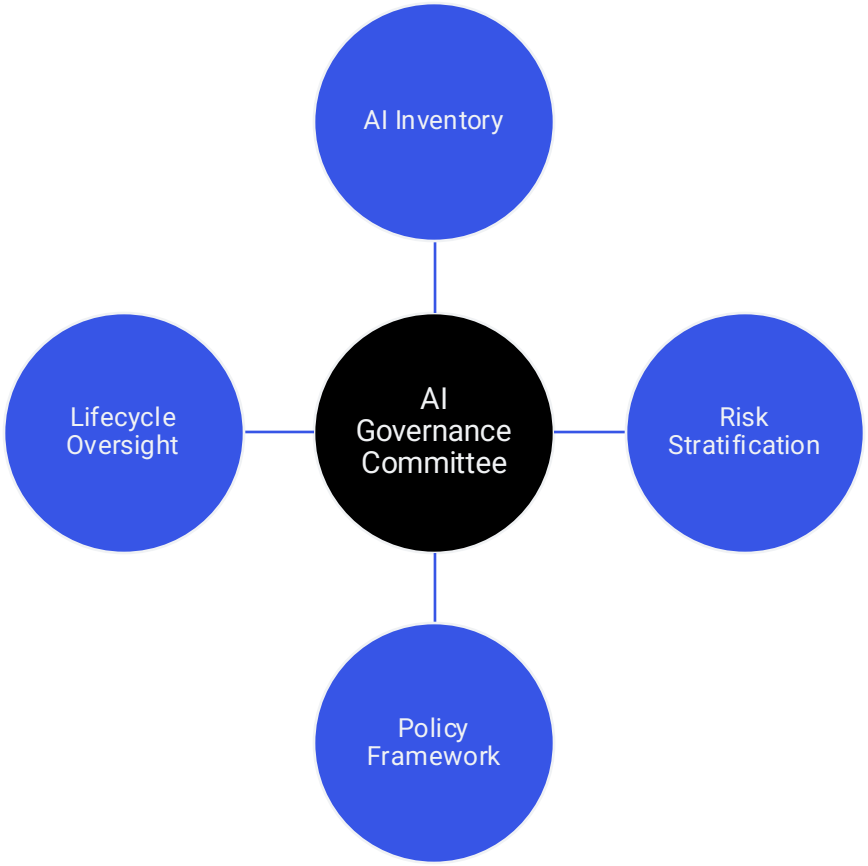
Clearwater

Today’s Mission

Understand the need to operationalize monitoring of AI to achieve **Safety** and **Transparency** and see how some healthcare organizations are doing it today.

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AI Inventory: Enables oversight, supports audits, and prevents untracked AI risks (e.g., outdated models).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

Clearwater COGNOME

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.

Address AI Governance Challenges to Ensure Trustworthy Healthcare AI

The NIST AI Risk Management Framework identifies characteristics of trustworthy AI systems.

Characteristic	Description
Valid and Reliable	Provides accurate consistent results.
Safe	Should not lead to endangerment of human life, health, property, or environment.
Secure and Resilient	Protects against adverse events and able to respond if one occurs.
Accountable and Transparent	Enables visibility into how the system works and when it doesn't work, including an understanding of responsibilities associated with unintended or bad outcomes.
Explainable and Interpretable	Provides clarity on how the system works and the meaning of the outcome.
Privacy-enhanced	Considers the controls needed to safeguard human autonomy, identity, and dignity.
Fair with Harmful Bias Managed	Ensures that concerns around equality and equity are addressed.

Source: NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)

Prioritize Monitoring to Tackle AI Safety and Transparency

Monitoring AI performance is a cornerstone of governance, addressing the critical need for visibility and explainability in healthcare.

Examples	Description	Example
Performance Drift	Undermines Reliability: AI models can degrade, leading to inaccurate predictions.	Model drift in predictive analytics misguides decisions.
Black-Box Decisions	Erode Trust: Clinicians need clear insights into AI reasoning to validate outputs.	Opaque models risk misdiagnosis if uninterpretable.
Bias Detection	Requires Continuous Oversight: Real-time monitoring is essential to identify and mitigate biases.	Biased outputs can exacerbate health inequities.

Predictive vs Generative AI

Even though the concept of AI has existed since at least the 1950s, the public release of ChatGPT, a generative AI, and its obvious potential has gained a considerable amount of public attention driving AI up the hype curve.

Type of AI	Objective and Function	Example Uses
Predictive AI	• Objective: Predictive AI focuses on analyzing historical data to forecast future outcomes or classify future events. It provides actionable insights and aids in decision-making and strategy formulation. • Functionality: It employs machine learning algorithms such as regression, classification, and time series analysis to recognize patterns and make predictions based on existing data.	• Hospital Readmission Prediction • Disease Progression Forecasting • Sepsis Detection • Resource Allocation Optimization • Medication Adherence Prediction
Generative AI	• Objective: The primary goal of generative AI is to create new and original content. This includes generating text, images, music, and other media by learning from existing data patterns. • Functionality: It uses sophisticated models like Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) to learn patterns and distributions from existing data, enabling the generation of new samples that exhibit creativity and originality.	• Synthetic Medical Image Generation • Drug Discovery • Personalized Treatment Plans • Clinical Note Generation • Virtual Health Assistants • Medical Education Simulations

Key Considerations for Trustworthy AI

Are your models running locally or remotely?

Do you governance capabilities to manage your portfolio of models?

Have your models been trained on your own data?

Are models integrated into clinical workflow and have you opened the AI/ML “black box”?

Clearwater COGNOME

Strategic Priorities for Responsible AI Adoption

Ensure Alignment with Clinical, Operational, Research and Business Priorities

Unified Approach for AI Governance and Adoption

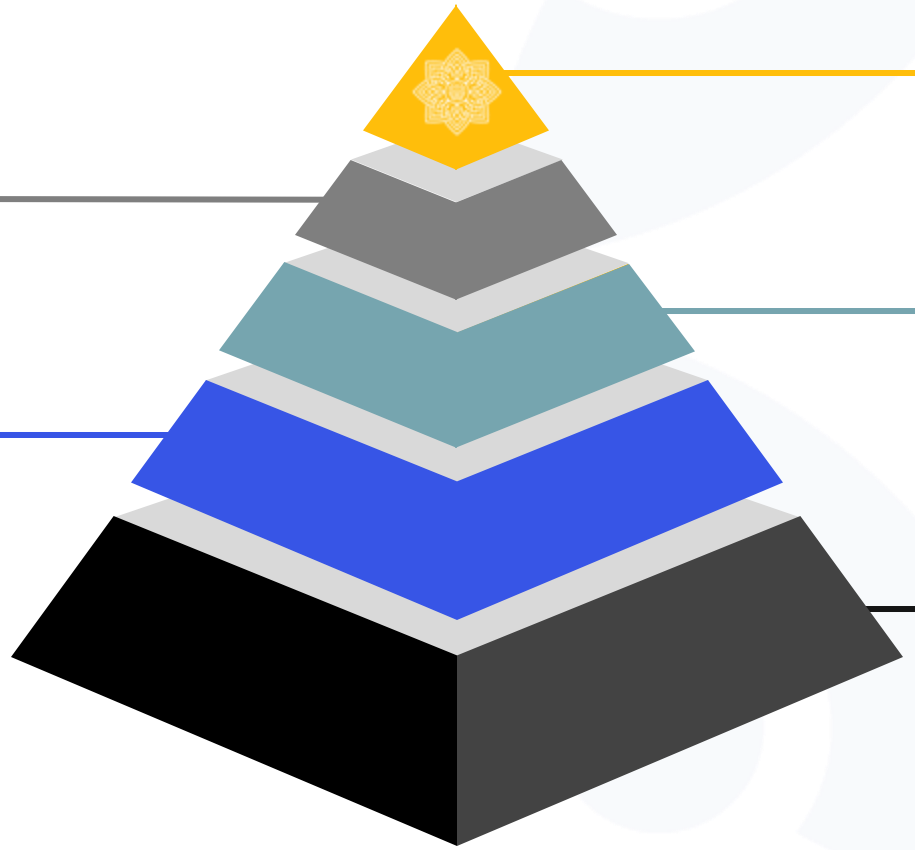
AI Strategy & Roadmap

Demonstrable ROI for AI Investments

Develop AI and Data Science Expertise

Clearwater COGNOME

A Framework for Unified AI Governance



ExplainerAI™
Continuous Governance

AI/ML Ops

- **Development**
- **Implementation**
- **Optimization**

Health System Data Sources

Gen AI Apps & ML Models

Alignment to Regulatory Frameworks

Clearwater COGNOME

Demo Time

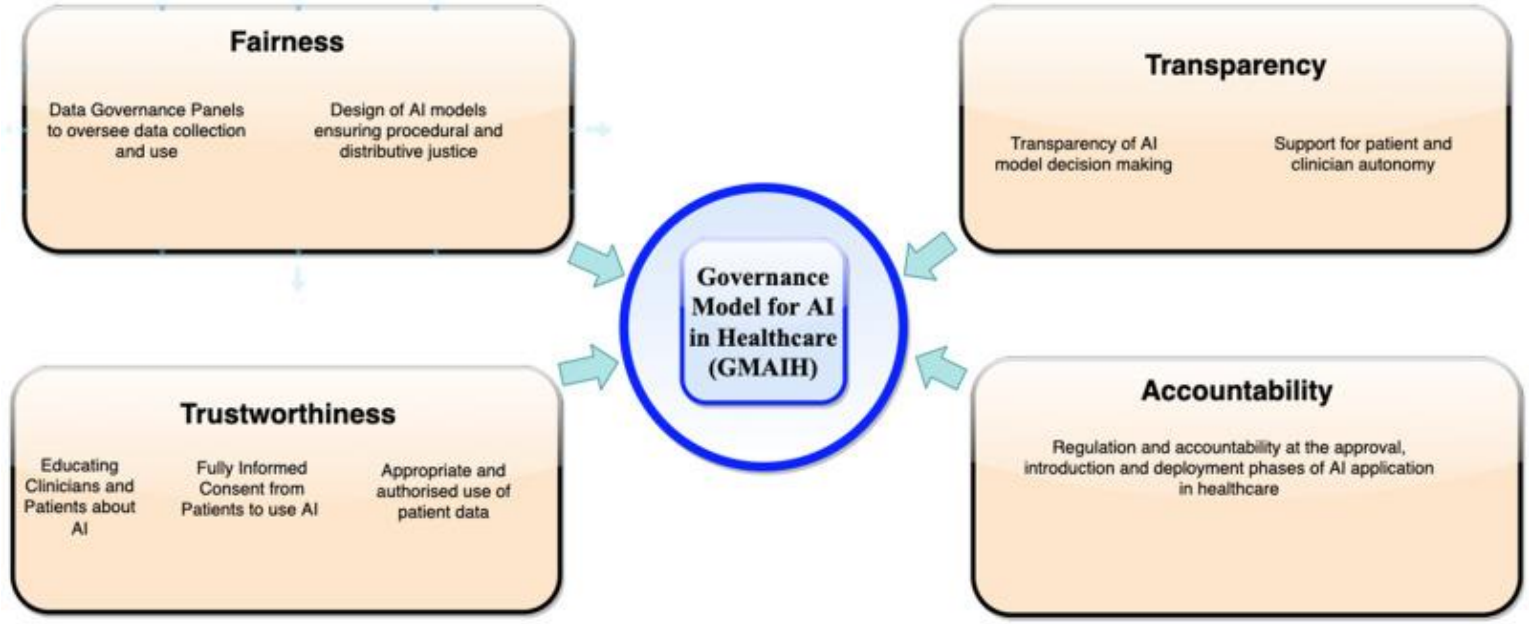
COGNOME

(Machine) Learning Healthcare

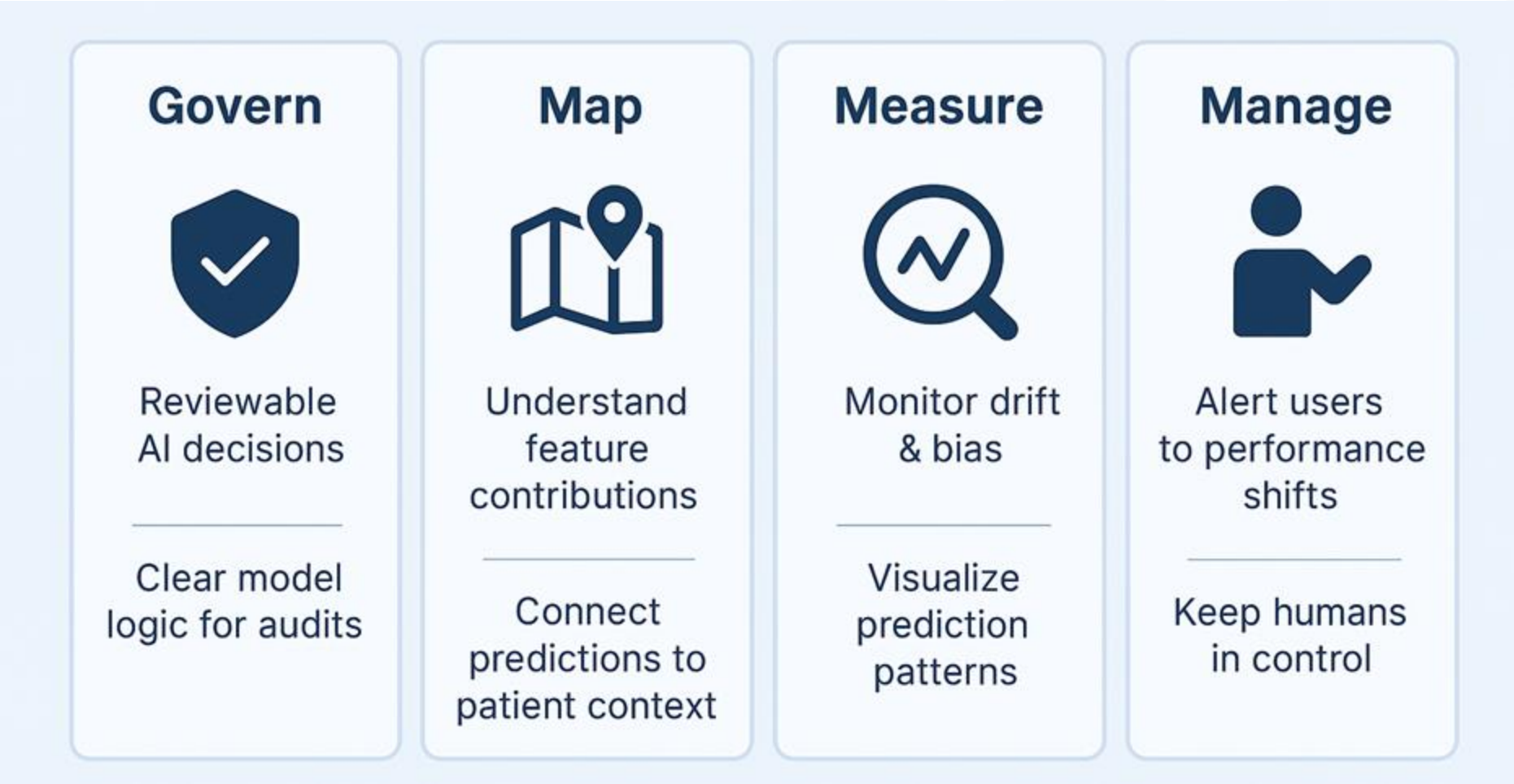
NIH Governance Model for Healthcare AI

Key Principles

- Understand Your Data Training Sets
- Integrate within Clinical and Operational Workflows
- Clinician & Patient Trust: Transparency is Key
- Monitor for Bias/Equity/Fairness
- Optimize models to prevent “Drift” and “Hallucinations”
- Enhance Cybersecurity, Privacy & Consent Policies & Practices
- Ensure Regulatory Compliance: NIST AI Risk Management Framework



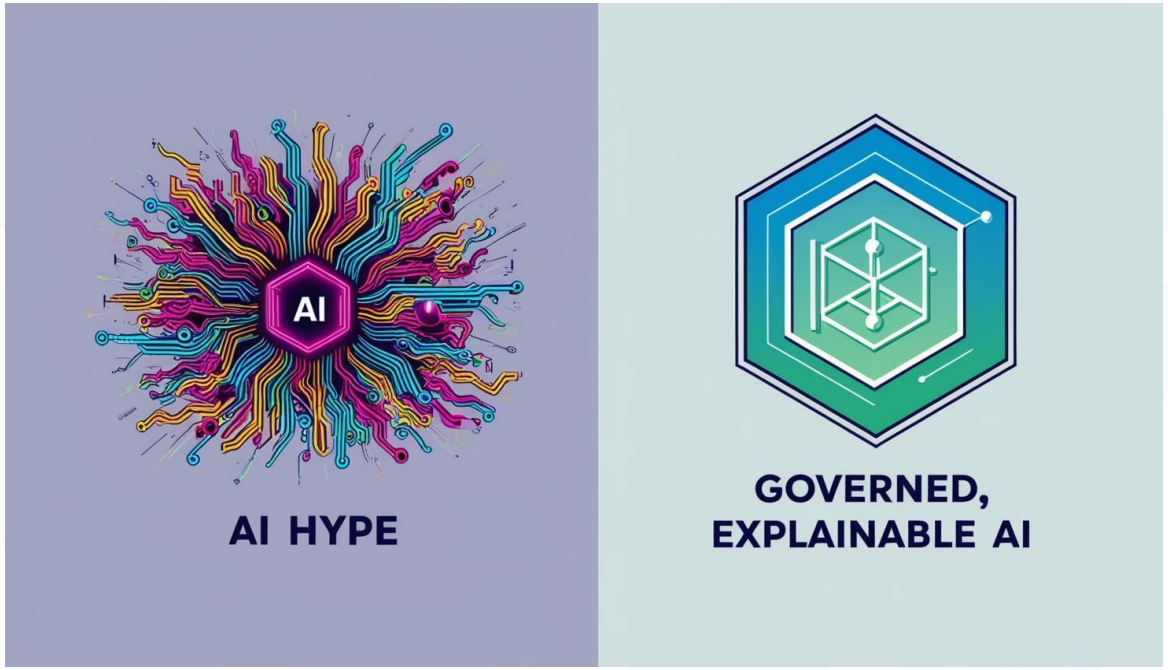
NIST AI Risk Management Framework (RMF)



Clearwater COGNOME

Governance “Must-Dos”

- Ensure Transparency
- Spot Hallucinations, Bias, and Model Drift early
- Explain ML Decisions at the Patient Level
- Align with NIH & NIST frameworks
- Foster Governance through Trust



Clearwater COGNOME

Q&A

Contact Information

E: jon.moore@clearwatersecurity.com

Jon Moore, MS, JD, CHISL, HCISPP

Chief Risk Officer & SVP
Consulting Services
Clearwater

E: james.green@cognome.com

James Green

Chief Executive Officer
Cognome

Clearwater

Tomorrow's Agenda – Day 2

June 24

11:00 am – 11:45 am CT
The State of AI Regulation in Healthcare



12:00 am – 12:45 pm CT
AI, Privacy, and the Future of Healthcare:
Legal Perspectives with Thomas Nachbar


1:00 pm – 1:45 pm CT
The Compliance Officer's Guide to Managing the Use of AI


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.