# Audit-Ready for the Colorado AI Act?

## Most Healthcare Organizations Aren’t, Not Yet

*What the Colorado Artificial Intelligence Act actually demands, and why FDA clearance, vendor contracts, and good intentions aren’t enough*

A White Paper from Asher Informatics Leadership

January 2026

**Authors:**
Charlotte Kalafut, CEO & Co-Founder
John F. Kalafut, PhD, CTO & Co-Founder

# Executive Summary

On May 17, 2024, Colorado Governor Jared Polis signed the Colorado Artificial Intelligence Act (CAIA) into law, creating the first comprehensive AI regulation in the United States which was to take effect February 1, 2026.  In August 2025 the effective date was pushed to **June 30, 2026**. Its activation precedes even the EU AI Act's go live. This legislation imposes significant obligations on organizations that develop or deploy high-risk AI systems, with healthcare explicitly named as a regulated domain.

For healthcare organizations deploying clinical AI solutions, the compliance requirements are substantial: risk management programs, annual impact assessments, consumer disclosure obligations, and ongoing monitoring for algorithmic discrimination. Many organizations have spent 12-18 months of preparation using traditional approaches and still aren't sure they're completely ready. Even those prepared for CAIA lack confidence in their ability to adapt to other emerging standards and regulations.

**The Asher Informatics AI Governance Policy Studio changes this equation entirely.**

Our agentic configuration engine enables healthcare organizations to generate compliant governance frameworks, risk management policies, and impact assessment process steps in hours rather than months. Perhaps even more importantly, the Studio supports operating in the constantly evolving legal and risk landscape. Built specifically for clinical AI governance and aligned with the NIST AI Risk Management Framework, the platform provides the documentation, processes, and enabling tools like continuous monitoring capabilities that the Colorado AI Act demands.

# Key Colorado AI Act Requirements of Note

Unlike previous patchwork approaches, CAIA establishes a comprehensive framework that addresses the entire lifecycle of high-risk AI systems.

## What Makes AI Systems "High-Risk"

Under CAIA, a high-risk AI system is any system that makes, or is a substantial factor in making, a "consequential decision". It is defined as a decision with material, legal, or similarly significant effect in specific domains. Healthcare services are explicitly included in this definition. This means virtually every clinical AI deployment falls under CAIA's regulatory scope. Note, some may misunderstand the law and think that if an AI Application has been granted market authorization by the US FDA, then there are no obligations required of the "deployer" of these AI products, but it just isn't the case.

### Purchased (Off-the-Shelf) AI:

- **The Burden:** Even for purchased tools, the **Healthcare Organization (Deployer)** is legally responsible for conducting an impact assessment. They must verify that the vendor provided a "general statement" of use and performance metrics.
- **The Policy Gap:** Standard vendor contracts often lack the necessary governance clauses to ensure long-term compliance with Colorado's **"Duty of Care"** standard.
- **FDA Cleared Devices:** * While FDA clearance provides a clinical safety baseline, it **does not satisfy** Colorado's legal standard for "algorithmic discrimination" or "consumer notification" regarding high-risk decisions (e.g., triage prioritization or diagnostic bias).

### Bespoke (In-House) Tools:

- **Developer Obligations Apply:** If a hospital builds its own triage bot, they become a **Developer** under the law. This triggers **reporting requirements to the Attorney General** if algorithmic discrimination is discovered and requires intense dataset documentation.

### The Compliance Timeline

With enforcement beginning June 30, 2026, healthcare organizations face a narrow window to implement comprehensive governance programs. The Act's requirements are not optional suggestions as they establish legal obligations with enforcement authority vested in the Colorado Attorney General.

## Key Compliance Requirements for Healthcare Deployers

Healthcare organizations deploying AI systems face four primary compliance categories under CAIA:

### 1. Risk Management Policy and Program

Deployers must implement a documented risk management policy and program that specifies principles, processes, and personnel for identifying and mitigating algorithmic discrimination. The program must be iterative, regularly reviewed and updated, and demonstrate reasonableness, with explicit reference to alignment with the NIST AI Risk Management Framework.

### 2. Annual Impact Assessments

Within ninety days of deployment and annually thereafter, deployers must complete comprehensive impact assessments documenting: system purpose and use cases, algorithmic discrimination risk analysis, data categories processed, performance metrics and limitations, transparency measures, and post-deployment monitoring protocols. These assessments must be retained for at least three years after final deployment.

### 3. Consumer Rights and Disclosures

Before using AI for consequential decisions, deployers must provide patients with clear notice including: the system's purpose, the nature of decisions being made, contact information, plain-language system descriptions, and information about opt-out rights under the Colorado Privacy Act. When AI contributes to adverse decisions, additional disclosures are required, along with opportunities to correct data and appeal for human review.

### 4. Ongoing Monitoring and Notification

Deployers must conduct annual reviews to ensure systems are not causing algorithmic discrimination. If discrimination is discovered, notification to the Attorney General is required within ninety days. Public website disclosures must be maintained and periodically updated describing deployed systems and discrimination risk management practices.

## The Traditional Compliance Challenge

Healthcare organizations attempting to build CAIA compliance programs from scratch face formidable obstacles. Based on our analysis and industry consultations, traditional approaches require:

- **Legal review and policy drafting:** 3-6 months with specialized healthcare AI counsel
- **Impact assessment framework development:** 2-4 months to create templates and processes
- **Risk management program design:** 3-5 months to align with NIST AI RMF
- **Staff training and process implementation:** 2-3 months for organizational rollout
- **Monitoring infrastructure deployment:** 4-6 months for technical implementation

Total estimated timeline: 12-18 months. Total estimated cost for mid-sized health systems: $500,000-$1.5 million. For rural hospitals and community health centers, these requirements present potentially insurmountable barriers.

# The Asher Informatics Solution

The Asher Informatics AI Governance Policy Studio was purpose-built to solve this exact challenge. As part of the AshMatics Suite for clinical AI lifecycle management, our platform transforms months of manual compliance work into hours of guided configuration.

## Agentic Configuration Engine

At the heart of our solution is an intelligent agentic configuration engine that understands both regulatory requirements and healthcare operational realities. Through a structured interview process, the system captures your organization's specific context including deployed AI systems, clinical workflows, patient populations, and existing governance structures, and generates comprehensive, customized compliance documentation.

## NIST AI RMF Alignment

CAIA explicitly references the NIST AI Risk Management Framework as the benchmark for "reasonable care." Our platform maintains deep alignment with NIST AI RMF, automatically mapping your governance artifacts to framework requirements and generating the documentation needed to establish the rebuttable presumption of compliance that CAIA provides.

# From Statute to System:

## Operationalizing AI Governance in Clinical Environments

*Asher Informatics studio addresses the "Policy-to-Control" execution gap that organizations face when trying to move from broad state laws to actual clinical operations.*

Because the law requires **Impact Assessments** to be repeatable, annual, and updated within 90 days of substantial modifications. Your system automates the SOPs needed to ensure these assessments are not missed.

**Small Business Exemption Defense:** The law exempts deployers with <50 employees, but larger health systems do not get this pass. They need a **Policy Studio** to manage the complexity of varying tool risk tiers across thousands of employees.

**The Affirmative Defense:** The law allows an **affirmative defense** against Attorney General enforcement if a business can prove it follows a recognized **AI Risk Management Framework** (like NIST). Your platform's ability to map policies to NIST controls directly reduces legal liability.

**BUT:** The NIST AI RMF is guidance, not a standard. Contextualizing it for a healthcare delivery organization is no small task.  It can introduce more complexity than compliance actually requires.

Meeting the law demands operational context, technology-specific understanding, and practical tools for process steps like bias and discriminatory impact assessment. The AshMatics suite provides this context and is where we're receiving a lot of love.

## COMPLETE DOCUMENTATION SUITE

The Studio generates the complete documentation portfolio CAIA requires:

- Risk management policies tailored to your organizational structure
- Impact assessment templates pre-populated with your system information
- Consumer disclosure language appropriate for clinical contexts
- Monitoring and review protocols with defined responsibilities
- Incident response procedures for discrimination discovery
- Public disclosure documentation ready for website publication

# Why Months Not Years, Days Not Months

Our claim of significant time and cost saving for compliance enablement is grounded in three architectural advantages:

## Pre-Built Compliance Intelligence

The Policy Studio embeds comprehensive understanding of CAIA requirements, NIST AI RMF structures, healthcare regulatory context, and clinical AI deployment patterns. This intelligence—developed through extensive analysis of regulatory text, enforcement guidance, and healthcare AI governance best practices—eliminates the months of research and interpretation that traditional approaches require.

## Intelligent Customization

Rather than starting from blank templates, our agentic engine adapts proven governance frameworks to your specific context. The system asks the right questions, interprets your answers in your regulatory context, and generates documentation that reflects both compliance requirements and operational realities. What takes consultants weeks to produce, our platform generates in hours.

## Continuous Compliance Support

CAIA compliance is not a one-time achievement, it requires ongoing monitoring, annual assessments, and regular policy updates. The AshMatics Suite provides continuous compliance support, tracking deployed systems, flagging assessment deadlines, monitoring for discrimination indicators, and maintaining audit-ready documentation.

# Democratizing AI Governance

As a Public Benefit Corporation, Asher Informatics is committed to democratizing access to clinical AI governance capabilities. The Colorado AI Act's requirements should not create a two-tiered healthcare system where only well-resourced academic medical centers can safely deploy AI while rural hospitals and community health centers are left behind.

Our platform is specifically designed to serve healthcare organizations that need governance support most. Those without dedicated AI ethics teams, without seven-figure compliance budgets, and without armies of regulatory consultants. If you serve patients and deploy AI, you deserve access to governance tools that actually work.

# The Time to Act Is Now

June 30, 2026, is not far away. Healthcare organizations deploying clinical AI systems in Colorado or serving Colorado patients must begin compliance preparation now. The question is not whether to comply, but how to comply efficiently, effectively, and without disrupting the clinical AI initiatives that improve patient care.

The Asher Informatics AI Governance Policy Studio offers a clear path forward: comprehensive compliance enablement in hours rather than months, at a fraction of traditional consulting costs, with ongoing support that maintains your compliance posture as regulations evolve.

## Ready to Transform Your AI Governance Capabilities?

Contact Asher Informatics to schedule a demonstration of the AI Governance Policy Studio.

# About Asher Informatics

Asher Informatics PBC is a Pittsburgh-based healthcare AI governance company developing the AshMatics Suite for clinical AI lifecycle management. Founded by healthcare AI veterans with deep experience in medical imaging, clinical decision support, and regulatory compliance, Asher Informatics is dedicated to ensuring that the benefits of clinical AI reach every patient, in every community, deployed safely and responsibly.

**Charlotte Kalafut, CEO & Co-Founder,** brings extensive experience in healthcare technology development and startup leadership.

**John F. Kalafut, PhD, CTO & Co-Founder,** served as Chief Science Officer at GE Healthcare, where he led development of advanced clinical AI and medical imaging solutions deployed in healthcare systems worldwide.

**Disclaimer:** *This white paper is provided for informational purposes only and does not constitute legal advice. Organizations should consult qualified legal counsel regarding specific compliance obligations under the Colorado AI Act and related regulations.*