HINSHAW

AI Governance Expectations on the Rise for Insurers Amid New Regulatory Activity

NYDFS Highlights Frontier Risks, Colorado Redefines its AI Law, and NAIC Prepares Regulators with New Tools

Privacy, Cyber & AI Decoded Alert | 5 min read

Jun 5, 2026

By: Jason J. Oliveri, Cathy Mulrow-Peattie, Elyssa Eisenberg*

Insurance companies should treat recent developments in artificial intelligence (AI), privacy, and cybersecurity regulation as more than just policy signals. Regulators are moving toward examination-ready expectations for insurers' use of AI and automated decision-making technology, while cybersecurity regulators are warning that frontier AI may materially increase the speed and scale of cyber threats.

For insurers, the practical message is straightforward: AI governance is becoming part of cybersecurity and privacy compliance, market conduct oversight, claims handling, unfair discrimination analysis, and third-party risk management.

Key Developments

NYDFS Warns about Frontier AI Model Cybersecurity Risk

On May 21, 2026, the New York Department of Financial Services (NYDFS) issued an Advisory warning DFS-regulated entities that frontier AI models may amplify the "potency, scale, and speed" with which threat actors identify vulnerabilities and exploits in information systems.

DFS stated that the advisory does not impose new requirements. Still, it urged regulated entities to update risk assessments, accelerate vulnerability management, coordinate with critical third-party service providers, validate AI-generated code, strengthen monitoring, and ensure compliance with 23 NYCRR Part 500.

A key element of the advisory is that NYSDFS advised that regulated entities should assess whether additional cybersecurity measures are warranted to address heightened risks associated with Frontier AI Models. At the same time, DFS issued additional guidance on Measures Regulated Entities Should Consider in a Heightened Cybersecurity Threat Environment. This new Guidance provides key best practices on when to adopt a heightened risk posture due to such cybersecurity risks caused by technological changes and geopolitical risks.

NYDFS Enforcement Remains Focused on Operational Cybersecurity Compliance

The advisory follows a DFS April 2026 cybersecurity settlement involving alleged Part 500 violations relating to cybersecurity program regulatory gaps, such as compliance with Part 500's specific incident response, data retention controls, and notification requirements.

Although not an AI enforcement action, the settlement reinforces DFS's expectation that cybersecurity policies should be operationalized.

Colorado Rewrites its AI Law

On May 14, 2026, Colorado enacted SB26-189, replacing its prior high-risk AI framework with a narrower automated decision-making technology (ADMT) framework **effective January 1, 2027.**

The law reflects a transparency-focused approach and expressly includes insurance-related "consequential decisions." SB26-189 imposes more limited obligations on developers and deployers of covered ADMTs.

Developers must provide deployers with a general statement of information regarding the ADMT's intended use, training data, known limitations, instructions on human review, and must notify deployers of any material updates or modifications. Both developers and deployers are also required to retain records necessary to demonstrate compliance for at least three years.

For deployers, the law introduces consumer-facing obligations, including the requirement to provide clear notice when ADMT is used in consequential decisions and, where an adverse decision is reached, to provide additional disclosures, enable consumers to access and correct their data, and request meaningful human review.

NAIC is Building Examination Infrastructure

The National Association of Insurance Commissioners' (NAIC) AI Systems Evaluation Tool is being piloted by the following 12 states in 2026 and is expected to be considered for adoption at the 2026 Fall National Meeting:

- California
- Colorado
- Connecticut
- Florida

- Iowa
- Louisiana
- Maryland
- Pennsylvania
- Rhode Island
- Vermont
- Virginia
- Wisconsin

The tool is intended to help regulators assess insurer AI use, governance, risk mitigation, potentially high-risk models, and input data. This suggests insurers should prepare for more standardized AI-related questions across market conduct, financial analysis, and examinations.

California Adds Privacy and ADMT Obligations

The finalized California Consumer Privacy Act (CCPA) regulations address cybersecurity audits, risk assessments, automated decision-making technology, and insurance companies:

- Risk assessment obligations began **January 1, 2026;**
- Automated decision-making technology (ADMT) compliance begins **January 1, 2027**; and
- Cybersecurity audit certifications are phased in for larger businesses **beginning in 2028.**

Health Insurance AI Remains High Risk

Regulators, policymakers, and plaintiffs continue to focus on AI used in prior authorization, utilization review, claims administration, payment, and fraud detection.

Key themes include human review, individualized assessment, transparency, auditability, privacy limits on patient data use, and anti-discrimination controls.

Why These AI and Privacy Developments Matter for Insurers

These developments show that AI governance has moved from general principles to operational requirements. Insurers should expect regulators to ask where AI is used, what personal information supports it, which vendors are involved, how models are tested, how unfair discrimination is assessed, how outputs are reviewed, and how consumers are informed or afforded review when AI affects decisions.

The developments also show that AI risk is not limited to consumer-facing decision-making. AI may affect cybersecurity risk, software development, third-party dependencies, incident response, data retention, claims handling, and privacy compliance.

Key takeaway: Insurers that treat AI governance as a narrow innovation or technology issue may miss the broader regulatory exposure.

What Insurers Should Do Now

Insurers and insurance-related entities should consider taking the following steps to comply with AI and privacy regulations:

Inventory AI and ADMT Use Cases

- Identify AI, machine learning, predictive analytics, scoring tools, rules engines, automated decision trees, generative AI, chatbots, and other ADMT across underwriting, pricing, eligibility, claims, fraud, utilization review, marketing, customer service, producer management, and internal operations.

Prioritize High-Impact Decisions

- Determine which tools materially influence decisions affecting insurance access, eligibility, premiums, benefits, claim payment, claim denial, coverage modification, utilization review, fraud determinations, or other adverse outcomes.

Update Cybersecurity Risk Assessments, Internal Policies, and Practices

- DFS-regulated entities should assess whether frontier AI risks are reflected in Part 500 risk assessments, vulnerability management, monitoring, incident response, secure coding practices, third-party oversight, and resilience testing practices and policies.

Review Vendor and Third-Party Controls

- Contracts and oversight procedures should address model documentation, data provenance, data use restrictions, audit rights, performance testing, unfair discrimination testing, cybersecurity controls, change notice, incident notice, human review support, record retention, and, of course, indemnification for any failures.

Prepare Regulator-Facing Documentation

- Insurers should develop examination-ready AI governance materials, including AI inventories, model risk classifications, testing protocols, approval workflows, vendor oversight records, consumer complaint procedures, and documentation showing how AI outputs are reviewed and challenged.

Review Notices and Appeal Workflows

- Insurers should assess whether consumer notices, adverse action communications, utilization review letters, claim denial letters, appeal procedures, and human review processes are sufficient where AI or ADMT materially influences a decision.

Align AI Governance with Privacy and Data Minimization

- Companies should determine whether personal information used for AI training, scoring, profiling, fraud analysis, claims analytics, or utilization review is necessary, accurate, appropriately retained, and used consistently with privacy notices, consents, contractual restrictions, and applicable privacy laws.

Bottom Line for Insurers

Insurers should not wait for a government examination, an enforcement action, a consumer complaint, or a claim dispute before beginning this work.

A defensible AI governance program should be able to answer basic questions:

- where AI is used;
- what data supports it;
- which vendors are involved, and are there adequate regulatory contracts in place with these vendors;
- whether the tool affects underwriting, pricing, claims, utilization review, or other consequential decisions;
- how outputs are tested;
- how consumers can obtain review or correction where required; and
- how AI-related cybersecurity risks are identified and mitigated

---

**Elyssa Eisenberg is a law clerk and is not admitted to practice law.*

Related People

Cathy Mulrow-Peattie

Partner

212-655-3875

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Data Privacy, AI & Cybersecurity

Insurance

Insurance Coverage Litigation & Counseling

Insurance Regulatory & Compliance

Regulatory & Compliance

Website Data Privacy

Related Insights

6 Key Takeaways From the IAPP 2026 Global Summit for Privacy Compliance Professionals

Tags

Cyber, Privacy, Cybersecurity, & Artificial Intelligence