Colorado Draft AI Insurance Rules Are a Watershed for AI Governance Regulation

February 14, 2023

On February 1, 2023, the Colorado Division of Insurance ("DOI") released its draft Algorithm and Predicative Model Governance Regulation (the "Draft AI Regulation"). The Draft AI Regulation imposes requirements on Colorado-licensed life insurance companies that use external data and AI systems in insurance practices. This release follows months of highly active engagement between the DOI and industry stakeholders, resulting in a first-in-the-nation set of AI and Big Data governance rules that will influence state, federal and international AI regulations for many years to come.

As we discussed on our recent webcast, the Draft AI Regulation focuses on governance, policies, training and documentation. But in doing so, the regulation imposes significant operational requirements on regulated entities. For example, the regulation obligates companies to identify governance principles for AI, supervised by the Board, and managed by a cross-functional governance committee. Regulated entities then need to inventory the AI uses involving external data, create security controls, and monitor their AI usage. Finally, there are reporting requirements to the DOI. For companies that are not already far down this road, full compliance will be a significant endeavor.

These requirements are analogous to those in the NYDFS Cybersecurity Rules, and we anticipate they will have a similar impact as that regulation had six years ago. The NYDFS Cybersecurity Rules were extremely influential in cyber regulation because they took what were, up until that point, vague principles, such as "reasonable cybersecurity," and turned them into concrete requirements for policies, governance and technical controls, along with a mandatory annual certification of compliance. Once hundreds of companies in New York demonstrated that they could comply with the NYDFS cyber requirements, they became industry best practices, and other regulators implemented similar requirements.

The Draft AI Regulation may have a similar sway. Colorado has taken vague principles of AI ethics, such as accountability, fairness, transparency, etc., and turned them into the concrete requirements for policies, governance, and technical controls. In a recent call, stakeholders expressed that some of the requirements in the Draft AI Regulation

are overly prescriptive. The DOI did not concur, but the current comment period is an opportunity to point out to the DOI where a more principles-based approach would be more productive. This is especially important because, during that same stakeholders meeting, the DOI suggested that these rules, or very similar rules, will likely be applied to other insurance lines (*e.g.*, property, auto, and causality) and other AI and Big Data uses (*e.g.*, claims, fraud detection, and marketing).

Another reason the Draft AI Regulation is likely to be influential is its brevity. In a little more than four pages, it provides over two dozen specific requirements. Contrast that with the National Institute of Standards and Technology's ("NIST") Artificial Intelligence Risk Management Framework ("AI RMF") that was released on January 26, 2023, which provided all of the same requirements, but scattered over several different documents that total close to 65 pages. Similarly, the White House's Blueprint for an AI Bill of Rights, issued in October 2022, espouses many of the same principles as the Draft AI Regulation, but in a 73 page document. In short, NIST's AI RMF and the White House AI Bill of Rights provide a very long menu of possible requirements for regulators interested in tackling AI governance and compliance, while the DOI's Draft AI Regulation provides a concise set of concrete rules.

In this Debevoise Data Blog post, we discuss the Draft AI Regulation's requirements, its likely impact on AI regulatory landscape, and how companies can prepare for compliance.

Takeaways

- ***Comments***: Insurers should closely review the Draft AI regulation and consider providing comments before the February 28 deadline. In the lead-up to the adoption of the NYDFS Cybersecurity Rules, several significant changes were made to the draft regulations before they were final as a result of industry comments.

- ***Gap Analysis & Road Map:*** Insurers should consider conducting a gap analysis between the requirements in the Draft AI Regulation and their current AI and Big Data governance and compliance program. After the gap analysis, insurers should consider developing a road map to compliance. For some companies that are covered by the Regulation, it may take significant time and resources to fully implement these requirements, and so they may want to start early. And even companies that are not subject to the Draft AI Regulation may consider conducting a gap analysis in anticipation that these rules, or similar ones, are likely to be adopted by other regulators in the coming years, or will come to be considered best practices for AI governance and compliance programs.

- ***Cross-Functional Committee:*** The regulation calls for a cross-functional committee. It may be worthwhile to create such a committee soon to oversee the gap analysis and road map.

- ***Budget***: The Draft AI Regulations will likely take effect in 2023, and many components of its obligations will require some companies to significantly increase their compliance budgets. Companies should consider starting the process of securing additional resources, if needed, from senior management.

Overview of the Draft AI Regulation Requiring a Governance

Following the enactment of Colorado Senate Bill 21-169, the DOI began a series of stakeholder meetings to promote discussion with industry representatives, and provide transparency into the rulemaking process (covered here, here, and here). During the Stakeholder meeting on February 7, the DOI first discussed the Draft AI Regulation and facilitated public comment (due by February 28, 2023). After the comment period, the DOI will begin the formal rulemaking process.

The Draft AI Regulation requires covered entities to implement an AI governance and risk management framework that ensures that the use of External Consumer Data and Information Sources ("ECDIS") and algorithms and predictive models ("AI Model") using ECDIS in insurance practices does not result in disproportionately negative outcomes. ECDIS is information used by life insurers to supplement or supplant traditional underwriting factors. The term includes: credit scores, social media habits, purchasing habits, home ownership, education attainment, licensures, civil judgments, court records, occupation that does not have a direct relationship to mortality, morbidity or longevity risk, and insurance risk scores derived from the information listed or similar information.

A disproportionately negative outcome means "a result or effect that has been found to have a detrimental impact on a group as defined by race, color, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity, or gender expression, and that impact is material even after accounting for factors that define similarly situated consumers." Many will recognize this as an effort to define proxy discrimination. It is noteworthy that this particular definition of proxy discrimination does not appear to require any intention on the part of the insurer.

Measuring and assessing such a detrimental impact on some of these characteristics is likely to be challenging for insurers. How will insurers know if they are unintentionally discriminating on race, religion or sexual orientation, for example, if they do not collect

such data? While there are some semi-reliable methods for inferring race and ethnicity from other data points, like Bayesian Improved First Name Surname Geocoding (BIFSG), we are not aware of any method for inferring some of these other characteristics. Will insurers have to start collecting this kind of data from customers, at least in a limited way for testing purposes? This remains to be seen and is worth exploring through the comment process.

Governance and Risk Management Obligations in the Draft AI Regulation

Section 5 of the Draft AI Regulation sets out its core governance requirements:

- ***Guiding Principles***. The Draft AI Regulation requires that insurers using ECDIS and AI Models establish governing principles outlining their values and objectives that provide guidance for ensuring transparency and accountability, as well as preventing unfair discrimination. **Section 5(A)(1).**

- ***Board and Senior Management Oversight***. The board of directors and senior management must be responsible and accountable for "setting and monitoring the overall strategy" on the use of ECDIS and AI models, and provide direction on AI governance. Entities should facilitate "clear lines of communication" and regular reporting to senior management regarding model risks and performance. **Section 5(A)(2)**.

- ***Cross-Functional Governance Committee***. Insurers must establish a cross-functional committee that is composed of representatives from "key functional areas" including legal, compliance, risk management, product development, underwriting, actuarial, data science, marketing and customer service, as applicable. **Section 5(A)(3)**.

- ***Policies.*** Insurers must have written policies and processes for the design, development, testing, deployment, use and ongoing monitoring of ECDIS and algorithms that use ECDIS to ensure that they are documented, tested, and validated.

- ***Training***. Insurers must develop and implement an ongoing supervision and training program for relevant personnel on the responsible and compliant use of ECDIS that addresses issues related to bias and unfair discrimination. **Section 5(A)(6)**.

- ***Cybersecurity***. Insurers must have internal security controls in place to prevent unauthorized access to AI models. **Section 5(A)(7)**.

- ***AI Incident Response Plan***. Insurers must have a plan for responding to and recovering from any unintended consequences of AI usage, which may be similar to Incident Response Plans developed by companies to prepare for cybersecurity incidents. **Section 5(A)(9)**.

- ***Consumer Complaints and Inquiries***. Insurers must establish processes for addressing consumer complaints and inquiries about the use of AI Models in a manner that provides "sufficiently clear" information so that consumers can take meaningful action in the event of an adverse decision. **Section 5(A)(8)**.

- ***Audit Resources***. Insurers must engage outside experts to perform audits when internal resources are insufficient. **Section 5(A)(10)**.

- ***Vendor Risk Management***. If insurers use third-party vendors for their ECDIS and AI models, they remain responsible for ensuring compliance with the requirements in the Draft AI Regulation and must establish a process for the selection and oversight of these vendors. **Section 5(B)**; **6(A)(11)**.

Documentation Obligations

Section 6 of the Draft AI Regulation sets out a robust list of documentation requirements, which presuppose certain operational elements that many insurers will need to establish.

- ***Inventory of AI Models***. Insurers are required to maintain an up-to-date inventory of all ECDIS, algorithms and predictive models in use, which includes a detailed description of each, its purposes, the problems it is intended to solve, potential risks, appropriate safeguards, inputs and outputs of the models, limitations on the models, and details on the model's training sets (including size and source). **Section 6(A)(1), (5), (6), (8)**.

- ***Annual Inventory Review***. Insurers are required to document the results and timing of annual reviews of the AI model inventory, including the modification, decommissioning, or replacement of any ECDIS or AI model. **Section 6(A)(2)**.

- ***Bias Assessments***. Insurers must have a description of any testing conducted to detect unfair discrimination resulting from the use of ECDIS and AI models, including the methodology, assumptions, results and steps taken to address disproportionate negative outcomes.

- ***Monitoring***. Insurers must document ongoing monitoring regarding the performance of their AI models. **Section 6(A)(7)**.

- ***Decision-making***. Insurers must document decisions made regarding the use of ECDIS during the entire lifecycle of AI models using that data, including the individual responsible for each documented decision and their decision-making process. **Section 6(A)(12)**.

Certification of Compliance

Once the Draft AI Regulation goes into effect, entities using ECDIS with AI models will have six months to provide a report to the DOI summarizing the progress made towards implementing its requirements. After one year, these entities will be required to submit to the DOI a compliance certification, along with a detailed description of their compliance. Thereafter, a certification of compliance, along with supporting documentation, is required every two years.

Covered entities that do not use ECDIS are exempt from the reporting requirements. However, they are required to submit an attestation to the DOI stating that they do not use ECDIS within one month from the effective data of the regulations and annually thereafter.

To subscribe to the Data Blog, please click here.

The Debevoise Artificial Intelligence Regulatory Tracker (DART) is now available for clients to help them quickly assess and comply with their current and anticipated AI-related legal obligations, including municipal, state, federal, and international requirements.

* * *

Please do not hesitate to contact us with any questions.

We would like to thank law clerk Jackie Dorward for her contribution to this Debevoise In Depth.

NEW YORK


Eric Dinallo
edinallo@debevoise.com


Avi Gesser
agesser@debevoise.com


Erez Liebermann
eliebermann@debevoise.com


Marshal L. Bozzo
mlbozzo@debevoise.com


Samuel J. Allaman
sjallama@debevoise.com


Anna R. Gressel
argressel@debevoise.com


Melissa Muse
mmuse@debevoise.com