DEPARTMENT OF REGULATORY AGENCIES

DIVISION OF INSURANCE

3 CCR 702-4

LIFE, ACCIDENT AND HEALTH

DRAFT PROPOSED New Regulation XX-XX-XX

GOVERNANCE AND RISK MANAGEMENT FRAMEWORK REQUIREMENTS FOR LIFE INSURANCE CARRIERS' USE OF EXTERNAL CONSUMER DATA AND INFORMATION SOURCES, ALGORITHMS, AND PREDICTIVE MODELS

Section 1 Authority

This regulation is promulgated and adopted by the Commissioner of Insurance under the authority of §§ 10-1-109, C.R.S. and 10-3-1104.9, C.R.S.

Section 2 Scope and Purpose

This regulation establishes the governance and risk management requirements for ~~a~~ life insurers that use ~~insurance company's internal governance and risk management framework necessary to ensure that life insurers' use of~~ external consumer data and information sources (ECDIS), as well as algorithms~~,~~ and predictive models that use ECDIS.~~does not result in unfairly discriminatory insurance practices.~~

Section 3 Applicability

This regulation shall apply to all life insurers authorized to do business in the state of Colorado.

Section 4 Definitions

A. "Algorithm" shall have the same meaning as set forth in § 10-3-1104.9, C.R.S.

~~B. "Disproportionately Negative Outcome" means, for the purpose of this regulation, 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.~~

B~~C~~. "Division" means, for the purposes of this regulation, the Colorado Division of Insurance.

CD. "External Consumer Data and Information Source" or "ECDIS" means, for the purposes of this regulation, a data or an information source that is used by a life insurer to supplement or supplant traditional underwriting factors or other insurance practices or to establish lifestyle indicators that are used in insurance practices. This term includes credit scores, social media habits, locations, purchasing habits, home ownership, educational attainment, licensures, civil judgments, court records, occupation that does not have a direct relationship to mortality, morbidity or longevity risk, consumer-generated Internet of Things data, and any insurance risk scores derived by the insurer or third-party from the above listed or similar data and/or information source.

DE. "Insurance Practice" shall have the same meaning as set forth in § 10-3-1104.9. C.R.S.

EF. "Life Insurer" or "insurer" means, for the purpose of this regulation, an entity authorized and licensed by the commissioner of insurance to sell, solicit, and issue life insurance products in the state of Colorado.

FG. "Predictive Model" shall have the same meaning as set forth in § 10-3-1104.9, C.R.S.

H. Traditional Underwriting Factors" means, for the purpose of this regulation, the following factors:

1. Medical information, family history, occupational, disability, or behavioral information related to a specific individual, which information, based on sound actuarial principles, has a direct relationship to mortality, morbidity, or longevity risk;

2. Income, assets, or other elements of a specific person's financial profile that a life insurer may use to determine insurable interest, suitability or eligibility for coverage; or

3. Digitized or other electronic forms of the information listed above such as electronic medical and prescription drug records.

GI. "Unfairly Discriminate" and "Unfair Discrimination" shall have the same meaning as set forth in § 10-3-1104.9, C.R.S.

Section 5 Governance and Risk Management Framework

A. Life insurers that use ECDIS, as well as algorithms and predictive models that useing ECDIS in an insurance practice must establish a risk-based governance and risk management framework that facilitates and supports policies, procedures, and systems designed to determine whether the use of such ECDIS, algorithms, and predictive models are credible in all material respects and their use in any insurance practice does not result in unfair discrimination with respect to race. The governance and risk management framework must include the following components:

1. Documented governing principles outlining the values and objectives of the insurer that:

   a. Provide the guidance necessary for ensuring that ECDIS, and algorithms and predictive models that useing ECDIS are designed, developed, used, and monitored in a manner that is well-suited for effective oversight and management is transparent, and accountable,; and;

   b. Ensure that the use of ECDIS, and the algorithms and predictive models that useing ECDIS do not lead to unfair discrimination;

2. Board of directors or appropriate Board committee oversight of the risk management framework;and s

3. Senior management responsibility and accountability for setting and monitoring the overall strategy~~,~~ and providing direction for governance on the use of ECDIS, and algorithms and predictive models that use~~ing~~ ECDIS. This includes established clear lines of communication and regular reporting to senior management on the performance and potential risks of ECDIS, algorithms, and predictive models that use ECDIS;

4~~3~~. Cross-functional algorithm and predictive model governance group~~committee~~ composed of representatives from key functional areas including legal, compliance, risk management, product development, underwriting, actuarial, data science, marketing, and customer service, as applicable;

~~4. Clearly assigned and documented roles and responsibilities of key personnel involved in the design, development, use, and oversight of ECDIS, and algorithms and predictive models using ECDIS;~~

5. Established written policies and processes, including assigned roles and responsibilities, for the design, development, testing, deployment, use, selection and oversight of vendors, and ongoing monitoring of ECDIS and algorithms and predictive models that use ECDIS and to ensure that they are documented, tested, and validated. Such policies and processes shall include an ongoing supervision and training program for relevant personnel on the responsible and compliant use of ECDIS, algorithms, and predictive models that use ECDIS;

~~6. Development and implementation of an ongoing supervision and training program for relevant personnel on the responsible and compliant use of ECDIS, algorithms, and predictive models including issues related to bias and potential unfair discrimination;~~

~~7. Implementation of controls to prevent unauthorized access of an algorithm or predictive model;~~

6~~8~~. Processes and protocols in place for addressing consumer complaints and inquiries about the use of ECDIS, as well as algorithms, and predictive models that use ECDIS in a manner that provides consumers with sufficiently clear information necessary for consumers to take meaningful action in the event of an adverse decision;

~~9. Plan for responding to and recovering from any unintended consequences; and~~

~~10. Engage outside experts for performing audits when internal resources are insufficient ;~~

7. Rubric for assessing and prioritizing risks associated with the deployment of ECDIS, as well as algorithms and predictive models that use ECDIS, in insurance practices with appropriate consideration given to consumer impact(s);

8. An up-to-date inventory, including version control, of all utilized ECDIS, as well as algorithms, and predictive models that use ECDIS, including a detailed description of each ECDIS, algorithm, and predictive model, their clearly stated purpose(s), and the outputs generated through their use;

9. Documented explanation of any material change(s) in the inventory of all ECDIS, as well as all algorithms and predictive models that use ECDIS and the rationale for the change(s);

10. Documented description of testing conducted to detect unfair discrimination in insurance practices resulting from the use of ECDIS, as well as algorithms and predictive models

that use ECDIS including the methodology, assumptions, results, and steps taken to address unfairly discriminatory outcomes;

11. Documented description of ongoing monitoring regarding the performance of algorithms and predictive models that use ECDIS;

12. Documented description of the process used for selecting external resources including third-party vendors that supply ECDIS, algorithms, and/or predictive models that use ECDIS including the intended use of the ECDIS, algorithm(s), and/or predictive model(s); and

13. Insurers must conduct regular reviews of the governance structure and risk management framework and make appropriate updates to the required documentation to ensure its continued accuracy and relevance.

B. If an insurer uses third-party vendors and other external resources with respect to ECDIS as well as algorithms and predictive models that use ECDIS, the insurer remains responsible for ensuring all regulatory requirements are met, including the production of any documents or information that the Division deems necessary to ensure compliance with regulatory requirements, and must establish a process for the selection and oversight of all external resources and third-party vendors as part of the governance and risk management framework and documented therein.

C. All components of the governance structure and risk management framework required by Section 5 must be available upon request by the Division pursuant to § 10-3-1104.9(4), C.R.S.

~~**Section 6 Documentation**~~

~~A. Life insurers must maintain comprehensive documentation for their use of all ECDIS and algorithms and/or predictive models that use ECDIS including all ECDIS, algorithms, and predictive models supplied by third-parties. At minimum, documentation must include:~~

~~1. An up-to-date inventory of all ECDIS, algorithms, and predictive models in use, including a detailed description of each ECDIS, algorithm, and predictive model, their clearly stated purpose(s), and the problem(s) their use is intended to solve and any potential risks and appropriate safeguards;~~

~~2. Results and timing of annual reviews of the inventory including the modification, decommissioning, or replacement of any ECDIS, and algorithms and/or predictive models using ECDIS and the rationale for modifying, decommissioning, or replacing any ECDIS, and algorithms and/or predictive models using ECDIS;~~

~~3. A system for tracking and managing changes to ECDIS, algorithms, and predictive models over time, including version control;~~

~~4. Description of testing conducted to detect unfair discrimination in insurance practices resulting from the use of ECDIS, algorithms, and predictive models including the methodology, assumptions, results, and steps taken to address disproportionate negative outcomes;~~

~~5. Description of the input and output of the algorithm and/or predictive model;~~

~~6. Description of any limitations of the algorithm and/or predictive model including situations in which it is not applicable or may not perform well;~~

7. Description of ongoing monitoring regarding the performance of an algorithm or predictive model;

8. Description of the dataset used to train an algorithm or model including its size, source, and any other relevant characteristics;

9. Description of how the algorithm or model makes predictions including any assumptions or simplifications made;

10. Identification of potential risks and impacts on applicants, policyholders, and insureds as well as the benefits;

11. Description of the process used for selecting external resources including third-party vendors;

12. All decisions made regarding the use of ECDIS and during the entire life cycles of all algorithms and/or predictive models using ECDIS including, at a minimum, the following:

a. The individuals responsible for making each documented decision;

b. The rationale and considerations behind each decision regarding the design, testing, deployment, operation, and performance as well as any constraints on their use;

c. Any relevant data, resources, or research used to inform each decision, and any potential consequence or impact of the decision;

d. Any changes to previously made decisions, including the rationale for the change(s) and the newly acquired or updated information that influenced the decision to make the change(s);

e. Evaluation of the use of third-party ECDIS, algorithms, and/or predictive models;

f. A description of the decision-making process and the individual(s) responsible for making each decision; and

g. Engagement of external resources and third-party vendors.

B. Insurers must conduct regular reviews and updates to the documentation to ensure its continued accuracy and relevance; and

C. All documentation must be easily accessible to appropriate insurer personnel and available upon request by the Division.

Section 6~~7~~ Reporting Requirements

A. Insurers that are using ECDIS as well as algorithms and/or predictive models that use~~ing~~ ECDIS as of the effective date of this regulation must submit to the Division a narrative report summarizing the progress made towards complying with the requirements specified in Section~~s~~ 5 ~~and 6. This report must also specifically~~ including identifying the areas still under development, any difficulties encountered, and expected completion date. This report is due six months following the effective date of this regulation.

B. Insurers that are using ECDIS as well as algorithms and/or predictive models that use~~ing~~ ECDIS as of the effective date of this regulation must submit to the Division ~~a report~~ one year following

the effective date of this regulation and annually thereafter a narrative report summarizing compliance with the requirements in Section 5 and the title of each individual responsible for ensuring compliance along with the specific requirement(s) from Section 5 for which that individual is responsible. This report must be signed by an officer attesting to compliance with this regulation. In the event an insurer is unable to attest to compliance with this regulation, the insurer must submit to the Division a corrective action plan.~~demonstrating compliance with Sections 5 and 6 one year following the effective date of this regulation. This report must contain the following elements:~~

~~1. Principles required in Section 5.A.1.;~~

~~2. Description of senior management responsibilities required by Section 5.A.2.;~~

~~3. Description of the team required by Section 5.A.3.;~~

~~4. The personnel and their roles and responsibilities required by Section 5.A.4.;~~

~~5. Policies and processes required by Section 5.A.5.;~~

~~6. Description of the monitoring and training required by Section 5.A.6;~~

~~7. Description of the controls required by Section 5.A.7.;~~

~~8. Processes and protocol required by Section 5.A.8.;~~

~~9. Plan required by Section 5.A.9.;~~

~~10. Process and plan for selecting and overseeing of all external resources required by Section 5.B.; and~~

~~11. Up-to-date inventory of all ECDIS and algorithms and predictive models using ECDIS and all other requirements in Section 6.A.1.~~

~~C. Insurers must submit to the Division a report every two years following the submission of the report required in Section 7.B. This report must contain the following elements:~~

~~1. Up-to-date inventory of all ECDIS and algorithms and predictive models using ECDIS and all other requirements in Section 6.A.1.;~~

~~2. Results and timing of reviews, and all other requirements in Section 6.A.2.;~~

~~3. Description of any material changes to the governance and risk management framework since the report in Section 7.B. and the effect these changes have had on the insurer related to its use of ECDIS and algorithms and predictive models using ECDIS; and~~

~~4. Description of any risks detected related to the use of ECDIS, algorithms, and predictive models and the steps taken to mitigate those risks.~~

C~~D~~. Insurers that do not use ECDIS or algorithms and/or predictive models that us~~e~~~~ing~~ ECDIS are exempt from the requirements described in Section~~s~~ 5 ~~and 6~~ and must submit to the Division within one month of the effective date of this regulation and annually thereafter an attestation signed by an officer indicating that the insurer does not use ECDIS or algorithms and/or predictive models that use ~~using~~ ECDIS.

D~~E~~. Insurers that do not use ECDIS or algorithms and/or predictive models that use~~ing~~ ECDIS as of the effective date of this regulation but subsequently plan to use ECDIS or algorithms and/or predictive models that use~~ing~~ ECDIS must ~~first~~ submit to the Division the report specified in Section 6.B. prior to the use of ECDIS or algorithms and/or predictive models that use ECDIS and annually thereafter. ~~7.B. Following the submission of the full report, insurers must submit a report to the Division in accordance with the requirements in Section 7.C.~~

Section 7 Confidentiality

Any documents or materials disclosed to the Division as a result of this regulation shall be subject to § 10-3-1104.9(3)(d), C.R.S.

Section 8 Severability

If any provision of this regulation or the application of it to any person or circumstance is for any reason held to be invalid, the remainder of this regulation shall not be affected.

Section 9 Enforcement

Noncompliance with this regulation may result in the imposition of any sanctions made available in the Colorado statutes pertaining to the business of insurance, or other laws, which include the imposition of civil penalties, issuance or cease and desist orders, and/or suspensions or revocations of license, subject to the requirements of due process.

Section 10 Effective Date

This regulation shall become effective on month, day, 2023.

Section 11 History

New Regulation Effective month, day, 2023.