

# DEPARTMENT OF REGULATORY AGENCIES

## Division of Insurance

### 3 CCR 702-10

#### UNFAIR DISCRIMINATION

##### Amended Regulation 10-1-1

#### **GOVERNANCE AND RISK MANAGEMENT FRAMEWORK REQUIREMENTS FOR LIFE INSURERS', PRIVATE PASSENGER AUTOMOBILE INSURERS', AND HEALTH BENEFIT PLAN INSURERS' USE OF EXTERNAL CONSUMER DATA AND INFORMATION SOURCES, ALGORITHMS, AND PREDICTIVE MODELS**

Section 1	Authority
Section 2	Scope and Purpose
Section 3	Applicability
Section 4	Definitions
Section 5	Governance and Risk Management Framework
Section 6	Reporting Requirements
Section 7	Confidentiality
Section 8	Severability
Section 9	Enforcement
Section 10	Effective Date
Section 11	History

##### **Section 1 Authority**

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

##### **Section 2 Scope and Purpose**

This regulation establishes the governance and risk management requirements for insurers authorized to do business in Colorado and offering individual life insurance, private passenger automobile insurance, and/or health benefit plans that use external consumer data and information sources (ECDIS), as well as algorithms and predictive models that use ECDIS, in any insurance practice.

##### **Section 3 Applicability**

This regulation shall apply to all insurers authorized to do business in the state of Colorado and offering the following types of insurance:

- A. Individually issued life insurance;
- B. Private passenger automobile insurance; and
- C. Health benefit plans.

##### **Section 4 Definitions**

- A. "Algorithm" shall have the same meaning as set forth in § 10-3-1104.9(8)(a), C.R.S.

- B. "Covered Person" shall have the same meaning as set forth in § 10-16-102(15), C.R.S.
- C. "Division" means, for the purposes of this regulation, the Colorado Division of Insurance.
- D. "External Consumer Data and Information Source" or "ECDIS" means, for the purposes of this regulation:
1. For life insurers, a data or an information source that is used by the 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, biometric data, and any insurance risk scores derived by the insurer or third-party from the above listed or similar data and/or information sources.
  2. For private passenger automobile insurers, a data or an information source that is used by the 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, consumer-generated Internet of Things data including telematics data, biometric data, and any insurance risk scores derived by the insurer or third-party from the above listed or similar data and/or information sources.
  3. For health benefit plan insurers, a data or an information source that is used by the 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, consumer-generated Internet of Things data, biometric data, and any insurance risk scores derived by the insurer or third-party from the above listed or similar data and/or information sources. For health benefit plan insurers, ECDIS does not include an individual's medical records.
- E. "Health Benefit Plan" shall have the same meaning as set forth in § 10-16-102(32), C.R.S.
- F. "Health Care Service" shall have the same meaning as set forth in § 10-16-102(33), C.R.S.
- G. "Insurance Practice" shall have the same meaning as set forth in § 10-3-1104.9(8), C.R.S.
- H. "Insurer" shall have the same meaning as set forth in § 10-1-202(6), C.R.S.
- I. "Internet of Things" means, for the purposes of this regulation, networks of physical objects embedded with sensors, software, and other technologies for the purposes of collecting, transmitting, and exchanging data over the Internet. This definition does not apply to devices that require direct human intervention for data collection and exchange.
- J. "Life Insurer" means, for the purpose of this regulation, an entity authorized and licensed by the commissioner of insurance to sell life insurance products in the state of Colorado.
- K. "Private Passenger Automobile Insurer" means, for the purpose of this regulation, an entity authorized and licensed by the commissioner of insurance to sell private passenger automobile insurance products in the state of Colorado.

- L. "Provider" shall have the same meaning as set forth in § 10-16-102, C.R.S.
- M. "Predictive Model" shall have the same meaning as set forth in § 10-3-1104.9, C.R.S.
- N. "SERFF" means, for the purpose of this regulation, System of Electronic Rate and Form Filing.
- O. "Unfairly Discriminate" and "Unfair Discrimination" shall have the same meaning as set forth in § 10-3-1104.9(8)(e), C.R.S.

## **Section 5      Governance and Risk Management Framework**

- A. Insurers that offer products listed in Section 3 and that use ECDIS, as well as algorithms and predictive models that use ECDIS in any insurance practice, must establish a risk-based governance and risk management framework that facilitates and supports policies, procedures, systems, and controls designed to determine whether the use of such ECDIS, algorithms, and predictive models potentially result in unfair discrimination with respect to race and remediate unfair discrimination, if detected through quantitative testing requirements established by the Division. The governance and risk management framework must include the following components:
  - 1. Documented governing principles outlining the values and objectives of the insurer that provide the guidance necessary for ensuring that:
    - a. ECDIS, and algorithms and predictive models that use ECDIS are designed, developed, used, and monitored in a manner that achieves effective oversight and management; and
    - b. The use of ECDIS, and the algorithms and predictive models that use ECDIS are reasonably designed to prevent unfair discrimination.
  - 2. The governance structure and risk management framework must be overseen by the board of directors or a committee of the board.
  - 3. Senior management responsibility and accountability for setting and monitoring the overall strategy and providing direction governing the use of ECDIS, and algorithms and predictive models that use ECDIS. This includes establishing clear lines of communication and delegated decision-making authority, and regular reporting to senior management on the performance and potential risks of using ECDIS, and the algorithms and predictive models that use ECDIS.
  - 4. Documented cross-functional ECDIS, algorithm, and predictive model governance group composed of representatives from key functional areas including legal, compliance, risk management, product development, underwriting, actuarial, data science, marketing, and customer service, as applicable.
  - 5. Health benefit plan insurers shall ensure that a provider acting on behalf of the insurer is ultimately responsible for the decisions made when ECDIS, or algorithms or predictive models that use ECDIS, are used to inform decisions to modify, or deny requests by a covered person or a covered person's provider for authorization prior to, or concurrent with, the provision of health care services to a covered person.
  - 6. Documented policies, processes, and procedures, including assigned roles and responsibilities, for the design, development, testing, deployment, use, and ongoing monitoring of ECDIS, as well as algorithms and predictive models that use ECDIS, and processes to ensure that they are documented, tested, and validated. Such policies and

processes must ensure the ECDIS is credible, relevant, and appropriate for its intended purpose or the intended purpose of the algorithm or predictive model and include an ongoing internal supervision and training program for relevant personnel on the responsible and compliant use of ECDIS, and the algorithms and predictive models that use ECDIS.

7. Documented processes and protocols in place for addressing applicant, policyholder, beneficiary, or covered person complaints and inquiries about the use of ECDIS, as well as algorithms and predictive models that use ECDIS. Such policies and protocols must provide the applicant, policyholder, beneficiary, or covered person with information necessary to take meaningful action in the event of an adverse decision made based on the use of ECDIS, and the algorithms and predictive models that use ECDIS. Carriers may use existing procedures for grievances and appeals.
  8. Documented policies, procedures, and processes 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 reasonable consideration given to the insurance practices' impacts on applicants, policyholders, beneficiaries, or covered persons.
  9. Documented 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.
  10. 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).
  11. Documented description of quantitative testing conducted pursuant to requirements established by the Division 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.
  12. Documented description of ongoing monitoring regarding the performance of algorithms and predictive models that use ECDIS including accounting for model drift.
  13. 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).
  14. Documented comprehensive annual reviews of the governance structure and risk management framework and 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 requirements in Section 5.A. are met, including the production of any documents or information that the Division deems necessary to ensure compliance with regulatory requirements. The insurer must establish and document a process for the selection and oversight of all external resources and third-party vendors as part of the governance structure and risk management framework.

Insurers may satisfy requests for documentation and information by third-party vendors providing the requested documents or information directly to the Division on behalf of the insurer.

- C. For life insurers, 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. on December 1, 2024, and annually thereafter. For private passenger automobile and health benefit plan insurers, all components of the governance structure and risk management framework required by Section 5 must be available upon request by the Division on July 1, 2026, and annually thereafter.

## **Section 6      Reporting Requirements**

- A. Insurers that offer products listed in Section 3 and that are using ECDIS, as well as algorithms and/or predictive models that use 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 5 including identifying the areas still under development, any difficulties encountered, and expected completion date. This report is due June 1, 2024, for life insurers and December 1, 2025, for private passenger automobile insurers and health benefit plan insurers.
- B. Life insurers that are using ECDIS, as well as algorithms and/or predictive models that use ECDIS, as of the effective date of this regulation must submit to the Division on December 1, 2024 and annually thereafter a report summarizing compliance with the requirements in Section 5 and the title and qualifications of each individual responsible for ensuring compliance along with the specific requirement(s) from Section 5 for which that individual is responsible.
- C. Private passenger automobile insurers and health benefit plan insurers that are using ECDIS, as well as algorithms and/or predictive models that use ECDIS, as of the effective date of this regulation must submit to the Division on July 1, 2026 and annually thereafter a report summarizing compliance with the requirements in Section 5 and the title and qualifications of each individual responsible for ensuring compliance along with the specific requirement(s) from Section 5 for which that individual is responsible.
- D. As part of the reports required by Sections 6B and 6C, the names of each individual may also be provided but are unnecessary to comply with this requirement. These reports 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. This report shall be no more than ten (10) pages including an executive summary and address Sections 5.A.1. through 5.A.13.
- E. Insurers that do not use ECDIS or algorithms and/or predictive models that use ECDIS are exempt from the requirements described in Section 5 and must submit to the Division within one month of the effective date of this regulation and on December 1 annually thereafter an attestation signed by an officer indicating that the insurer does not use ECDIS or algorithms and/or predictive models that use ECDIS.
- F. Insurers that do not use ECDIS or algorithms and/or predictive models that use ECDIS as of the effective date of this regulation but subsequently plan to use ECDIS or algorithms and/or predictive models that use ECDIS must 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.
- G. All reports required by this Section 6 shall be submitted in SERFF using Annual Report as the filing type. Separate filings shall be used for each insurer. The filing description shall indicate that the report is being submitted pursuant to Colorado Insurance Regulation 10-1-1.

## **Section 7      Confidentiality**

Any documents or materials disclosed to the Division as a result of this regulation, including documents submitted in SERFF, 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 of cease and desist orders, and/or suspensions or revocations of license, subject to the requirements of due process.

## **Section 10      Effective Date**

This amended regulation shall become effective on October 15, 2025.

## **Section 11      History**

New regulation effective November 14, 2023.  
Amended regulation effective October 15, 2025.