

DEPARTMENT OF REGULATORY AGENCIES

Division of Insurance

CONSUMER PROTECTION (GENERAL)

3 CCR 702-6

[Editor's Notes follow the text of the rules at the end of this CCR Document.]

Regulation 6-1-1 CONCERNING LIMITATION OF COVERAGE

Section 1	Authority
Section 2	Scope and Purpose
Section 3	Applicability
Section 4	Definitions
Section 5	Rules
Section 6	Severability
Section 7	Enforcement
Section 8	Effective Date
Section 9	History

Section 1 Authority

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

Section 2 Scope and Purpose

The purpose of this regulation is to establish rules for the conditions to be met by all life and health insurers and carriers issuing policies, riders, endorsements, and amendments which limit the coverage usually and normally afforded. It is the responsibility of all insurers and carriers to see that all purchasers of policies issued by them are fully informed as to the coverages provided in those policies, the specific premiums charged, and for any limitations, exceptions, or exclusions for which coverage is not provided.

Section 3 Applicability

This regulation shall apply to all life insurers issuing life insurance policies subject to the laws of Colorado. It also applies to all carriers offering policies of accident and sickness coverage subject to the laws of Colorado.

Section 4 Definitions

- A. "Carrier" shall have the same meaning as found at § 10-16-102(8), C.R.S.
- B. "Policy of sickness and accident insurance" shall have the same meaning as found at § 10-16-102(50), C.R.S.

Section 5 Rules

Any riders, endorsements, or amendments which limit coverage afforded by an existing policy shall not be effective unless and until the named insured or primary policyholder has signified his or her acceptance thereof by placing his or her signature on the proposed rider, endorsement, or amendment. One signed and dated copy must be attached to the policy.

Section 6 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 7 Enforcement

Noncompliance with this regulation may result in the imposition of any of the 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 revocation of license, subject to the requirements of due process.

Section 8 Effective Date

This regulation shall become effective on October 15, 2015.

Section 9 History

This regulation was originally effective in 1974.
Amended Regulation 6-1-1 effective February 1, 2004.
Repealed and Repromulgated Regulation effective October 15, 2015.

Regulation 6-2-1 [Repealed eff. 06/01/2012]

**Regulation 6-3-1 CONCERNING THE USE OF INDEPENDENT MARKET CONDUCT
SURVEILLANCE PERSONNEL AND APPEAL PROCESS FOR FEES AND EXPENSES**

Section 1	Authority
Section 2	Scope and Purpose
Section 3	Applicability
Section 4	Definitions
Section 5	Rules
Section 6	Severability
Section 7	Enforcement
Section 8	Effective Date
Section 9	History

Section 1 Authority

This regulation is promulgated and adopted by the Commissioner of Insurance under the authority of §§ 10-1-109, 10-1-304, and 10-1-308, C.R.S.

Section 2 Scope and Purpose

The purpose of this regulation is to set forth requirements for the use of independent contract market conduct surveillance personnel and to provide a process for the appeal of fees and expenses charged by such surveillance personnel.

Section 3 Applicability

This regulation applies to all market conduct surveillance conducted under Article 1 of Title 10.

Section 4 Definitions

- A. "Commissioner" shall have the meaning as found at § 10-1-302(1), C.R.S.
- B. "Division" shall have the meaning as found at § 10-1-302(4), C.R.S.
- C. "Entity" shall have the meaning of: "company", as found at §§ 10-1-102(6) and 10-1-302(2), C.R.S.; "insurer", as found at § 10-1-102(13), C.R.S.; "carrier", as found at § 10-16-102(8), C.R.S.; "title insurance company" as found at § 10-11-102(10), C.R.S.; "contract seller" as found at § 10-15-102(6), C.R.S.; and "general provider" as as found at § 10-15-102(9), C.R.S..
- D. "Market Conduct Surveillance" shall have the meaning as found at § 10-1-302(7), C.R.S.
- E. "Market Conduct Surveillance Personnel" ("Surveillance Personnel") shall have the meaning as found at § 10-1-302(8) C.R.S.

Section 5 Rules

- A. Selection of Market Conduct Surveillance Personnel
 - 1. The Division may use independent contract market conduct surveillance personnel to perform market conduct surveillance of entities subject to this regulation using the following criteria:
 - a. Number and frequency of market conduct surveillance activities;
 - b. Workload and availability of Division staff;
 - c. Out-of-state travel requirements and location of the market conduct surveillance site;
 - d. Experience and background as an independent contractor;
 - e. Special expertise required for market conduct surveillance; and
 - f. Market issues requiring unanticipated market conduct surveillance.
 - 2. Preference will be given to Colorado domestic entities, and then to entities with Colorado regional home offices, in determining whether the market conduct surveillance will be conducted by state employee surveillance personnel rather than independent contract market conduct surveillance personnel.
- B. Appeal Process for Fees and Expenses of Independent Contract Market Conduct Surveillance Personnel
 - 1. An entity may contest the reasonability of the fees and/or expenses by filing an appeal with the Commissioner, with a copy to the independent market conduct surveillance personnel, within ten (10) calendar days after receipt of the surveillance personnel's billing. Such appeal must set forth the charges that are considered to be unreasonable and the basis for the claim.

2. The entity shall pay any non-contested fees and/or expenses to the independent contract surveillance personnel according to the independent contractor's invoice.
3. The Commissioner shall review the appeal from the entity within fourteen (14) calendar days after receipt of such appeal and shall notify the entity in writing of the findings. Charges under dispute shall not be due until the Commissioner has reviewed the appeal and has rendered written findings, which constitute final agency action.
4. If the Commissioner determines that the charges under dispute are reasonable and in accordance with guidelines maintained by the Commissioner, the entity shall issue payment for such charges to the independent contract market conduct surveillance personnel within fourteen (14) calendar days of being notified of the Commissioner's determination, and shall so notify the Commissioner.

Section 6 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 7 Enforcement

Noncompliance with this regulation may result in the imposition of any of the 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 revocation of license, subject to the requirements of due process.

Section 8 Effective Date

This amended regulation is effective on June 1, 2018.

Section 9 History

New regulation effective April 1, 1998.
Amended regulation effective August 31, 2005.
Amended regulation effective July 1, 2012.
Amended regulation effective June 1, 2018.

Regulation 6-3-2 CONCERNING THE USE OF INDEPENDENT CONTRACTORS FOR INFORMAL INVESTIGATIONS AND THE APPEAL PROCESS FOR EXPENSES

- | | |
|-----------|-------------------|
| Section 1 | Authority |
| Section 2 | Scope and Purpose |
| Section 3 | Applicability |
| Section 4 | Definitions |
| Section 5 | Rule |
| Section 6 | Severability |
| Section 7 | Enforcement |
| Section 8 | Effective Date |
| Section 9 | History |

Section 1 Authority

This regulation is promulgated under the authority of §§ 10-1-109 and 10-1-208, C.R.S.

Section 2 Scope and Purpose

This regulation sets the requirements for using independent contractors for informal investigations, and provides a process to appeal the expenses and fees charged by such independent contractors.

Section 3 Applicability

This regulation shall apply to informal investigations of all authorized and unauthorized insurers and producers that transact insurance business in Colorado.

Section 4 Definitions

“Informal Investigation” means, for the purposes of this regulation, a Division review, analysis, inquiry, and/or research into referrals, complaints, and/or inquiries to determine whether any violations of Colorado insurance law or Colorado insurance regulation have occurred. Informal investigations include, but are not limited to, Division reviews, analyses, and inquiries initiated as a result of an on-going, or completed financial or market conduct examination.

Section 5 Rule

- A. Insurers and producers may be investigated without advance notice when the Division determines that an immediate investigation of the insurer's or producer's books, records or business practices is necessary for the protection of insurance consumers.
- B. Selection of independent contractors to perform informal investigations
 - 1. Pursuant to Section § 10-1-208, C.R.S., the Division may contract with a person, corporation or entity having technical or subject matter expertise or skill and experience in investigative techniques to perform informal investigations.
 - 2. The contractor may be the same contractor that performed, or is performing, a financial or market conduct examination of an insurer or producer. If an informal investigation is conducted subsequent to, or simultaneously with, a financial or market conduct examination, the Division and the independent contractor shall execute a separate contract for the informal investigation. Payments to the contractor for the informal investigation are governed by this Regulation 6-3-2.
 - 3. When determining whether to use independent contractors for informal investigations, the Division will consider whether it has sufficient available resources with sufficient technical expertise to perform the informal investigation. To the extent practicable the Division shall attempt to allocate Division employees possessing the necessary expertise, skill or experience to perform the informal investigation before using an independent contractor.
- C. Travel requirements

In addition to fees, independent contractors shall be compensated for travel, meals and lodging in a manner that is reasonable and consistent with Colorado fiscal guidelines.

- D. Appeal process for expenses and fees of independent contractors
 - 1. Prior to an informal investigation, the Division shall provide the insurer or producer to be investigated with an estimate of costs, fees and/or expenses for the investigation.

2. Independent contractors conducting informal investigations are required to submit itemized invoices for fees and expenses to the Division for review and approval in accordance with guidelines maintained by the Division. After review and approval, the Division will forward the invoice to the insurer or producer for payment directly to the independent contractor.
3. Whenever an insurer or producer considers fees or expenses charged by an independent contractor to be unreasonable, the insurer or producer may contest the amount of fees and/or expenses charged by filing an appeal with the Commissioner within ten (10) calendar days after receipt of the independent contractor's billing from the Division. Such appeal must set forth the fees and/or expenses that are considered unreasonable and the basis for the claim. The insurer or producer shall simultaneously mail a copy of the appeal to the independent contractor. The Division shall also notify the independent contractor that an appeal has been filed.
4. The insurer or producer shall not delay payment of any non-contested fees and/or expenses pending the outcome of the appeal.
5. The independent contractor may respond to the appeal filed with the Commissioner, with a copy to the insurer or producer, no later than ten (10) calendar days after the date the Division notifies the independent contractor of the appeal. Failure to file a response shall not be considered an admission by the independent contractor of the allegations raised in the insurer's or producer's appeal. Insurers and producers may not file a reply to the independent contractor's response.
6. The Commissioner shall review the appeal from the insurer or producer and any independent contractor response within ten (10) calendar days after the last date for the independent contractor to file a response. The Commissioner shall notify the parties in writing of his or her findings.
7. If the Commissioner determines that some or all of the charges under dispute are reasonable and in accordance with the Division's guidelines, the insurer or producer shall promptly pay to the independent contractor all disputed charges approved by the Commissioner.
8. Disputed charges shall not be due until the Commissioner has reviewed the appeal and rendered written findings.
9. Undisputed charges shall be paid promptly and shall not be withheld pending the Commissioner's finding on disputed charges.
10. The Commissioner's written findings shall constitute a final agency action for purposes of judicial review pursuant to § 24-4-106, C.R.S.

Section 6 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 the regulation shall not be affected.

Section 7 Enforcement

Noncompliance with this regulation may result in the imposition of any of the 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 revocation of license, subject to the requirements of due process.

Section 8 Effective Date

This regulation is effective February 1, 2016.

Section 9 History

Original regulation effective December 1, 2005.

Amended regulation effective February 1, 2016.

Regulation 6-4-1 PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION

Section 1	Authority
Section 2	Scope and Purpose
Section 3	Applicability
Section 4	Definitions
Section 5	Initial Privacy Notice to Consumers Required
Section 6	Annual Privacy Notice to Customers Required
Section 7	Information to be Included in Privacy Notices
Section 8	Form of Opt Out Notice to Consumers and Opt Out Methods
Section 9	Revised Privacy Notices
Section 10	Privacy Notices to Group Policyholders
Section 11	Delivery
Section 12	Limitation on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties
Section 13	Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information
Section 14	Limits on Sharing Account Number Information for Marketing Purposes
Section 15	Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Service Providers and Joint Marketing
Section 16	Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions
Section 17	Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information
Section 18	When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 19	Authorizations
Section 20	Authorization Request Delivery
Section 21	Rules
Section 22	Relationship to Colorado Laws
Section 23	Protection of Fair Credit Reporting Act
Section 24	Nondiscrimination
Section 25	Incorporation by Reference
Section 26	Severability
Section 27	Enforcement
Section 28	Effective Date
Section 29	History
Appendix A	Sample Clauses
Appendix B	Federal Model Privacy Form

Section 1 Authority

This regulation is promulgated and adopted by the Commissioner of Insurance under the authority of §§ 10-1-108, 10-1-109, 10-5-117, 10-16-109, and 10-16-401(4)(o), C.R.S.

Section 2 Scope and Purpose

This regulation governs the treatment of nonpublic personal health information and nonpublic personal financial information about individuals by all licensees of the Colorado Division of Insurance. This regulation:

- A. Requires a licensee to provide notice to individuals about its privacy policies and practices;
- B. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties; and
- C. Provides methods for individuals to prevent a licensee from disclosing that information.

Section 3 Applicability

- A. This regulation applies to:
 - 1. Nonpublic personal financial information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This regulation does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and
 - 2. All nonpublic personal health information.
- B. A licensee domiciled in Colorado that is in compliance with this regulation in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.
- C. Rules of Construction.

The examples in this regulation, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this regulation are not exclusive. Compliance with an example or use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this regulation. Licensees may rely on use of the Federal Model Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the privacy notice content requirements of this regulation. Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this regulation and/or the sample clauses in Appendix A, provided that such notices accurately describe the licensee's privacy practices and otherwise meet the notice content requirements of this regulation. However, while licensees may continue to use privacy notices that contain the examples in this regulation and/or the sample clauses in Appendix A, licensees may not rely on use of privacy notices with the sample clauses in Appendix A as a safe harbor of compliance with the notice content requirements of this regulation after July 1, 2019.

Section 4 Definitions

- A. "Affiliate" means, for the purpose of this regulation, any company that controls, is controlled by, or is under common control with another company.
- B. "Carrier" shall have the same meaning as found at § 10-16-102(8) C.R.S.

- C. “Clear and conspicuous” means, for the purpose of this regulation, that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice. Examples:
1. A licensee makes its notice reasonably understandable if it:
 - a. Presents the information in the notice in clear, concise sentences, paragraphs, and sections;
 - b. Uses short explanatory sentences or bullet lists whenever possible;
 - c. Uses definite, concrete, everyday words and active voice whenever possible;
 - d. Avoids multiple negatives;
 - e. Avoids legal and highly technical business terminology whenever possible; and
 - f. Avoids explanations that are imprecise and readily subject to different interpretations.
 2. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:
 - a. Uses a plain-language heading to call attention to the notice;
 - b. Uses a typeface and type size that are easy to read;
 - c. Provides wide margins and ample line spacing;
 - d. Uses boldface or italics for key words; and
 - e. In a form that combines the licensee’s notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.
 3. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page, if necessary, to view the entire notice and ensures that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:
 - a. Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or
 - b. Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.
- D. “Collect” means, for the purpose of this regulation, to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.
- E. “Commissioner” means, for the purpose of this regulation, the insurance commissioner of the state of Colorado.

- F. "Company" means, for the purpose of this regulation, a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.
- G. "Consumer" means, for the purpose of this regulation, an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative. Examples:
1. An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.
 2. An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.
 3. An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.
 4. An individual is a licensee's consumer if:
 - a. The individual is a beneficiary of a life insurance policy underwritten by the licensee;
 - b. The individual is a claimant under an insurance policy issued by the licensee;
 - c. The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or
 - d. The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and
 - e. The licensee discloses nonpublic personal financial information about the individual to a nonaffiliated third party other than as permitted under Sections 15, 16 and 17 of this regulation.
 5. Provided that the licensee provides the initial, annual and revised notices under Section 10 of this regulation to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about an individual described in subparagraphs a., b. or c. below, other than as permitted under Sections 15, 16, and 17 of this regulation, such an individual is not the consumer of the licensee solely because he or she is:
 - a. A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;
 - b. Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or
 - c. A claimant covered by a workers' compensation plan.

6. The individuals described in Section 4.G.5. are consumers of a licensee if the licensee does not meet all the conditions of Section 4.G.5.
 7. In no event shall the individuals, solely by virtue of the status described in Section 4.G.5. be deemed to be customers for purposes of this regulation.
 8. An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.
 9. An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.
- H. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).
- I. "Control" means, for the purpose of this regulation:
1. Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;
 2. Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or
 3. The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.
- J. "Customer" means, for the purpose of this regulation, a consumer who has a customer relationship with a licensee.
- K. "Customer relationship" means, for the purpose of this regulation, a continuing relationship between a consumer and a licensee under which the licensee provides one or more insurance products or services to the consumer that are to be used primarily for personal, family or household purposes. Examples:
1. A consumer has a continuing relationship with a licensee if:
 - a. The consumer is a current policyholder of an insurance product issued by or through the licensee; or
 - b. The consumer obtains financial, investment or economic advisory services relating to an insurance product or service from the licensee for a fee.
 2. A consumer does not have a continuing relationship with a licensee if:
 - a. The consumer applies for insurance but does not purchase the insurance;
 - b. The licensee sells the consumer airline travel insurance in an isolated transaction;
 - c. The individual is no longer a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee;

- d. The consumer is a beneficiary or claimant under a policy and has submitted a claim under a policy choosing a settlement option involving an ongoing relationship with the licensee;
 - e. The consumer is a beneficiary or a claimant under a policy and has submitted a claim under that policy choosing a lump sum settlement option;
 - f. The customer's policy is lapsed, expired, or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than annual privacy notices, material required by law or regulation, communication at the direction of a state or federal authority, or promotional materials;
 - g. The individual is an insured or an annuitant under an insurance policy or annuity, respectively, but is not the policyholder or owner of the insurance policy or annuity; or
 - h. For the purposes of this regulation, the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.
- L. "Financial institution" means, for the purpose of this regulation, any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). Financial institution does not include:
 - 1. Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.);
 - 2. The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.); or
 - 3. Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.
- M. "Financial product or service" means, for the purpose of this regulation, any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.
- N. "Health care" means, for the purposes of this regulation:
 - 1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests or counseling that:
 - a. Relates to the physical, mental or behavioral condition of an individual; or

- b. Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs or any other tissue; or
 - 2. Prescribing, dispensing or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.
- O. "Health care provider" means, for the purpose of this regulation, a physician or other health care practitioner licensed, accredited or certified, to perform specified health services consistent with state law, or a health care facility.
- P. "Health information" means, for the purpose of this regulation, any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:
 - 1. The past, present or future physical, mental or behavioral health or condition of an individual;
 - 2. The provision of health care to an individual; or
 - 3. Payment for the provision of health care to an individual.
- Q. "Insurance product or service" means, for the purpose of this regulation, any product or service that is offered by a licensee pursuant to the insurance laws of Colorado, including a Health Maintenance Organization or a Nonprofit Hospital, Medical-Surgical, and Health Service Corporation. Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for an insurance product or service.
- R. "Insurer" shall have the same meaning as found at § 10-1-102(13), C.R.S.
- S. "Licensee" means, for the purpose of this regulation, all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the insurance laws of Colorado.
 - 1. A licensee is not subject to the notice and opt out requirements for nonpublic personal financial information set forth in Sections 1 through 17 of this regulation if the licensee is an employee, agent or other representative of another licensee ("the principal") and:
 - a. The principal otherwise complies with, and provides the notices required by, the provisions of this regulation; and
 - b. The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this regulation.
 - 2. Examples of employee, agent or other representative of a principal:
 - a. An insurance producer, public adjuster or other licensee who is employed by another insurance producer, public adjuster or other licensee;
 - b. An insurance producer of an insurer;
 - c. An insurance producer that has binding authority for an insurer; or
 - d. A sublicensee of a licensee, whether or not the sublicensee is licensed in any other capacity.

3. Subject to Section 4.Q.2., "licensee" as defined in this regulation shall also include an unauthorized insurer that accepts business placed through a licensed surplus lines broker in Colorado, but only in regard to the surplus lines placements placed pursuant to § 10-5-108, C.R.S.
 4. A surplus lines broker or surplus lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal financial information set forth in Sections 1 through 17 of this regulation provided:
 - a. The broker or insurer does not disclose nonpublic personal information of a consumer or a customer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 145 of this regulation, except as permitted by Section 16 or 17 of this regulation; and
 - b. The broker or insurer delivers a notice to the consumer at the time a customer relationship is established on which the following is printed in 16-point type:

Privacy Notice

"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."
- T. "Nonaffiliated third party" means, for the purpose of this regulation, any person except:
1. A licensee's affiliate; or
 2. A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person). Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).
- U. "Nonpublic personal information" means, for the purpose of this regulation, nonpublic personal financial information and nonpublic personal health information.
- V. "Nonpublic personal financial information" means, for the purpose of this regulation:
1. Personally identifiable financial information; and
 2. Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
 3. Nonpublic personal financial information does not include:
 - a. Health information;
 - b. Publicly available information, except as included on a list described in Section 4.T.2.; or

- c. Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.
 - 4. Examples of lists.
 - a. Nonpublic personal financial information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.
 - b. Nonpublic personal financial information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.
- W. "Nonpublic personal health information" means, for the purpose of this regulation, health information:
 - 1. That identifies an individual who is the subject of the information; or
 - 2. With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.
- X. "Personally identifiable financial information" means, for the purpose of this regulation, any information:
 - 1. A consumer provides to a licensee to obtain an insurance product or service from the licensee;
 - 2. About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or
 - 3. The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.
 - 4. Examples.
 - a. Personally identifiable financial information includes:
 - (1) Information a consumer provides to a licensee on an application to obtain an insurance product or service;
 - (2) Account balance information and payment history;
 - (3) The fact that an individual is or has been one of the licensee's customers or has obtained an insurance product or service from the licensee;
 - (4) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

- (5) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;
 - (6) Any information the licensee collects through an internet cookie (an information-collecting device from a web server); and
 - (7) Information from a consumer report.
 - b. Personally identifiable financial information does not include:
 - (1) Health information;
 - (2) A list of names and addresses of customers of an entity that is not a financial institution; and
 - (3) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.
- Y. "Publicly available information" means, for the purpose of this regulation, any information that a licensee has a reasonable basis to believe is lawfully made available to the general public.
 - 1. That publically available information can be from:
 - a. Federal, state or local government records;
 - b. Widely distributed media; or
 - c. Disclosures to the general public that are required to be made by federal, state or local law.
 - 2. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:
 - a. That the information is of the type that is available to the general public; and
 - b. Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.
 - 3. Examples.
 - a. Publicly available information in government records includes information in government real estate records and security interest filings.
 - b. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.
 - c. A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

- d. A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

Section 5 Initial Privacy Notice to Consumers Required

- A. A licensee shall provide a clear and conspicuous initial notice that accurately reflects its privacy policies and practices to:
 - 1. Customer. An individual who becomes the licensee's customer, not later than when the licensee establishes a customer relationship, except as provided in Section 5.E. of this section; and
 - 2. Consumer. A consumer, before the licensee discloses any nonpublic personal financial information about the consumer to any nonaffiliated third party, if the licensee makes a disclosure other than as authorized by Sections 16 and 17.
- B. A licensee is not required to provide an initial notice to a consumer under Section 5.A.2. if:
 - 1. The licensee does not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by Sections 16 and 17, and the licensee does not have a customer relationship with the consumer; or
 - 2. A notice has been provided by an affiliated licensee, as long as the notice clearly identifies all licensees to whom the notice applies and is accurate with respect to the licensee and the other institutions.
- C. A licensee establishes a customer relationship at the time the licensee and the consumer enter into a continuing relationship. A licensee establishes a customer relationship when the consumer:
 - 1. Becomes a policyholder of a licensee that is an insurer when the insurer delivers an insurance policy or contract to the consumer, or in the case of a licensee that is an insurance producer or surplus line broker, obtains insurance through that licensee; or
 - 2. Agrees to obtain financial, economic or investment advisory services relating to insurance products or services for a fee from the licensee.
- D. When an existing customer obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Section 5. A. as follows:
 - 1. The licensee may provide a revised policy notice, under Section 9, that covers the customer's new insurance product or service; or
 - 2. If the initial, revised or annual notice that the licensee most recently provided to that customer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new privacy notice under Section 5. A.
- E. Exceptions to allow subsequent delivery of notice.
 - 1. A licensee may provide the initial notice required by Section 5. A.1. of this section within a reasonable time after the licensee establishes a customer relationship if:
 - a. Establishing the customer relationship is not at the customer's election; or

- b. Providing notice not later than when the licensee establishes a customer relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time.
 - 2. Examples of exceptions.
 - a. Establishing a customer relationship is not at the customer's election if a licensee acquires or is assigned a customer's policy from another financial institution or residual market mechanism and the customer does not have a choice about the licensee's acquisition or assignment.
 - b. Providing notice not later than when a licensee establishes a customer relationship would substantially delay the customer's transaction when the licensee and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the insurance product or service.
 - c. Providing notice not later than when a licensee establishes a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at the licensee's office or through other means by which the customer may view the notice, such as on a web site.
- F. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 11. If the licensee uses a short-form initial notice for non-customers according to Section 7.D., the licensee may deliver its privacy notice according to Section 7.D.3.

Section 6 Annual Privacy Notice to Customers Required

- A. General rule.
 - 1. A licensee shall provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship. Annually means at least once in any period of twelve (12) consecutive months during which that relationship exists. A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the customer on a consistent basis.
 - 2. Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the customer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a customer opens an account on any day of year 1, the licensee shall provide an annual notice to that customer by December 31 of year 2.
- B. Exception to general rule. A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections 15, 16, or 17 and has not changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or Section 5 shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any criteria described in this paragraph.
- C. Termination of customer relationship. A licensee is not required to provide an annual notice to a former customer. A former customer is an individual with whom a licensee no longer has a continuing relationship. Examples:

1. A licensee no longer has a continuing relationship with an individual if the individual no longer is a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee.
 2. A licensee no longer has a continuing relationship with an individual if the individual's policy is lapsed, expired or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than to provide annual privacy notices, material required by law or regulation, or promotional materials.
 3. For the purposes of this regulation, a licensee no longer has a continuing relationship with an individual if the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.
 4. A licensee no longer has a continuing relationship with a customer in the case of providing real estate settlement services, at the time the customer completes execution of all documents related to the real estate closing, payment for those services has been received, or the licensee has completed all of its responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.
- D. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 11.

Section 7 Information to be Included in Privacy Notices

- A. The initial, annual and revised privacy notices that a licensee provides under Sections 5, 6 and 9 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its privacy notice:
1. The categories of nonpublic personal financial information that the licensee collects;
 2. The categories of nonpublic personal financial information that the licensee discloses;
 3. The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information, other than those parties to whom the licensee discloses information under Sections 16 and 17;
 4. The categories of nonpublic personal financial information about the licensee's former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information about the licensee's former customers, other than those parties to whom the licensee discloses information under Sections 16 and 17;
 5. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 15. (and no other exception in Sections 16 and 17 applies to that disclosure), a separate description of the categories of information the licensee discloses and the categories of third parties with whom the licensee has contracted;
 6. An explanation of the consumer's right under Section 12.A. to opt out of the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

7. Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);
 8. The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and
 9. Any disclosure that the licensee makes under Section 6.B. of this section.
- B. Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under Sections 16 and 17, the licensee is not required to list those exceptions in the initial or annual privacy notices required by Sections 5 and 6. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.
- C. Examples.
1. Categories of nonpublic personal financial information that the licensee collects.
 - a. A licensee satisfies the requirement to categorize the nonpublic personal financial information it collects if the licensee categorizes it according to the source of the information.
 - b. A licensee shall categorize nonpublic personal information into the following categories, as applicable:
 - (1) Information from the consumer;
 - (2) Information about the consumer's transactions with the licensee or its affiliates;
 - (3) Information about the consumer's transactions with nonaffiliated third parties; and
 - (4) Information from a consumer reporting agency.
 2. Categories of nonpublic personal financial information a licensee discloses.
 - a. A licensee satisfies the requirement to categorize nonpublic personal financial information it discloses if the licensee categorizes the information according to source, as described in Section 6.C.1., as applicable, and provides a few examples to illustrate the types of information in each category. These might include:
 - (1) Information from the consumer, including application information, such as assets and income and identifying information, such as name, address and social security number;
 - (2) Transaction information, such as information about balances, payment history and parties to the transaction; and
 - (3) Information from consumer reports, such as a consumer's creditworthiness and credit history.

- b. A licensee does not adequately categorize the information that it discloses if the licensee uses only general terms, such as transaction information about the consumer.
 - c. If a licensee reserves the right to disclose all of the nonpublic personal financial information about consumers that it collects, the licensee may simply state that fact without describing the categories or examples of nonpublic personal information that the licensee discloses.
 - 3. Categories of affiliates and nonaffiliated third parties to whom the licensee discloses.
 - a. A licensee satisfies the requirement to categorize the affiliates and nonaffiliated third parties to which the licensee discloses nonpublic personal financial information about consumers if the licensee identifies the types of businesses in which they engage.
 - b. Types of businesses may be described by general terms only if the licensee uses a few illustrative examples of significant lines of business. For example, a licensee may use the term financial products or services if it includes appropriate examples of significant lines of businesses, such as life insurer, automobile insurer, consumer banking or securities brokerage.
 - c. A licensee also may categorize the affiliates and nonaffiliated third parties to which it discloses nonpublic personal financial information about consumers using more detailed categories.
 - 4. Disclosures under exception for service providers and joint marketers. If a licensee discloses nonpublic personal financial information under the exception in Section 15 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the licensee satisfies the disclosure requirement of Section 6.A.5. of this section if it:
 - a. Lists the categories of nonpublic personal financial information it discloses, using the same categories and examples the licensee used to meet the requirements of Section 6.A.2. of this section, as applicable; and
 - b. States whether the third party is:
 - (1) A service provider that performs marketing services on the licensee's behalf or on behalf of the licensee and another financial institution; or
 - (2) A financial institution with whom the licensee has a joint marketing agreement.
 - 5. If a licensee does not disclose, and does not wish to reserve the right to disclose, nonpublic personal financial information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under Sections 16 and 17, the licensee may simply state that fact, in addition to the information it shall provide under Section 6.A.1., 6.A.8., 6.A.9., and Section 6.B.
 - 6. A licensee describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal financial information if it does both of the following:

- a. Describes in general terms who is authorized to have access to the information; and
 - b. States whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses.
- D. Short-form initial notice with opt out notice for non-customers.
 - 1. A licensee may satisfy the initial notice requirements in Sections 5.A.2. and 8.C. for a consumer who is not a customer by providing a short-form initial notice at the same time the licensee delivers an opt out notice as required in Section 8.
 - 2. A short-form initial notice shall:
 - a. Be clear and conspicuous;
 - b. State that the licensee's privacy notice is available upon request; and
 - c. Explain a reasonable means by which the consumer may obtain that notice.
 - 3. The licensee shall deliver its short-form initial notice according to Section 11. The licensee is not required to deliver its privacy notice with its short-form initial notice. The licensee instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the licensee's short-form notice requests the licensee's privacy notice, the licensee shall deliver its privacy notice according to Section 11.
 - 4. The licensee provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the licensee:
 - a. Provides a toll-free telephone number that the consumer may call to request the notice; or
 - b. For a consumer who conducts business in person at the licensee's office, maintains copies of the notice on hand that the licensee provides to the consumer immediately upon request.
- E. The licensee's future disclosure notice may include:
 - 1. Categories of nonpublic personal financial information that the licensee reserves the right to disclose in the future, but does not currently disclose; and
 - 2. Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal financial information.
- F. Sample clauses illustrating some of the notice content required by this section and the Federal Model Privacy Form are included in Appendix A and Appendix B, respectively, of this regulation.

Section 8 Form of Opt Out Notice to Consumers and Opt Out Methods

- A. Form of opt out notice.

1. If a licensee is required to provide an opt out notice under Section 12.A., it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the right to opt out under that section. The notice shall state:
 - a. That the licensee discloses or reserves the right to disclose nonpublic personal financial information about its consumer to a nonaffiliated third party;
 - b. That the consumer has the right to opt out of that disclosure; and
 - c. A reasonable means by which the consumer may exercise the opt out right.
2. Examples.
 - a. A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal financial information to a nonaffiliated third party if the licensee:
 - (1) Identifies all of the categories of nonpublic personal financial information that it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which the licensee discloses the information, as described in Section 7.A.2. and 3., and states that the consumer can opt out of the disclosure of that information; and
 - (2) Identifies the insurance products or services that the consumer obtains from the licensee, either singly or jointly, to which the opt out direction would apply.
 - b. A licensee provides a reasonable means to exercise an opt out right if it:
 - (1) Designates check-off boxes in a prominent position on the relevant forms with the opt out notice;
 - (2) Includes a reply form together with the opt out notice;
 - (3) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's web site, if the consumer agrees to the electronic delivery of information; or
 - (4) Provides a toll-free telephone number that consumers may call to opt out.
 - c. A licensee does not provide a reasonable means of opting out if:
 - (1) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or
 - (2) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.
 - d. A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.
- B. A licensee may provide the opt out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 5.

- C. If a licensee provides the opt out notice later than required for the initial notice in accordance with Section 5, the licensee shall also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.
- D. Joint relationships.
 - 1. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt out notice. The licensee's opt out notice shall explain how the licensee will treat an opt out direction by a joint consumer (as explained in Section 8.D.5).
 - 2. Any of the joint consumers may exercise the right to opt out. The licensee may either:
 - a. Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or
 - b. Permit each joint consumer to opt out separately.
 - 3. If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all of the joint consumers.
 - 4. A licensee may not require all joint consumers to opt out before it implements any opt out direction.
 - 5. Example. If John and Mary are both named policyholders on a homeowner's insurance policy issued by a licensee and the licensee sends policy statements to John's address, the licensee may do any of the following, but it shall explain in its opt out notice which opt out policy the licensee will follow:
 - a. Send a single opt out notice to John's address, but the licensee shall accept an opt out direction from either John or Mary.
 - b. Treat an opt out direction by either John or Mary as applying to the entire policy. If the licensee does so and John opts out, the licensee may not require Mary to opt out as well before implementing John's opt out direction.
 - c. Permit John and Mary to make different opt out directions. If the licensee does so:
 - (1) It shall permit John and Mary to opt out for each other;
 - (2) If both opt out, the licensee shall permit both of them to notify it in a single response (such as on a form or through a telephone call); and
 - (3) If John opts out and Mary does not, the licensee may only disclose nonpublic personal financial information about Mary, but not about John and not about John and Mary jointly.
- E. A licensee shall comply with a consumer's opt out direction as soon as reasonably practicable after the licensee receives it.
- F. A consumer may exercise the right to opt out at any time.
- G. Duration of consumer's opt out direction.

1. A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.
 2. When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal financial information that the licensee collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the licensee, the opt out direction that applied to the former relationship does not apply to the new relationship.
- H. When a licensee is required to deliver an opt out notice by this section, the licensee shall deliver it according to Section 11.

Section 9 Revised Privacy Notices

- A. Except as otherwise authorized in this regulation, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section 5, unless:
1. The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;
 2. The licensee has provided to the consumer a new opt out notice;
 3. The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and
 4. The consumer does not opt out.
- B. Examples.
1. Except as otherwise permitted by Sections 15, 16 and 17, a licensee shall provide a revised notice before it:
 - a. Discloses a new category of nonpublic personal financial information to any nonaffiliated third party;
 - b. Discloses nonpublic personal financial information to a new category of nonaffiliated third party; or
 - c. Discloses nonpublic personal financial information about a former customer to a nonaffiliated third party, if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.
 2. A revised notice is not required if the licensee discloses nonpublic personal financial information to a new nonaffiliated third party that the licensee adequately described in its prior notice.
- C. When a licensee is required to deliver a revised privacy notice by this section, the licensee shall deliver it according to Section 11.

Section 10 Privacy Notices to Group Policyholders

Unless a licensee is providing privacy notices directly to covered individuals described in Section 4.G.5.a., b. or c., a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, in the manner described in Sections 5 through 9 of this regulation, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans.

Section 11 Delivery

- A. A licensee shall provide any notices that this regulation requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.
- B. A licensee may reasonably expect that a consumer will receive actual notice if the licensee:
 - 1. Hand-delivers a printed copy of the notice to the consumer;
 - 2. Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;
 - 3. For a consumer who conducts transactions electronically, posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;
 - 4. For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.
- C. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:
 - 1. Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or
 - 2. Sends the notice via electronic mail to a consumer who does not obtain an insurance product or service from the licensee electronically.
- D. A licensee may reasonably expect that a customer will receive actual notice of the licensee's annual privacy notice if:
 - 1. The customer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or
 - 2. The customer has requested that the licensee refrain from sending any information regarding the customer relationship, and the licensee's current privacy notice remains available to the customer upon request.
- E. A licensee may not provide any notice required by this regulation solely by orally explaining the notice, either in person or over the telephone.
- F. Retention or accessibility of notices for customers.

1. For customers only, a licensee shall provide the initial notice required by Section 5.A.1., the annual notice required by Section 6.A., and the revised notice required by Section 9 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.
2. A licensee provides a privacy notice to the customer so that the customer can retain it or obtain it later if the licensee:
 - a. Hand-delivers a printed copy of the notice to the customer;
 - b. Mails a printed copy of the notice to the last known address of the customer; or
 - c. Makes its current privacy notice available on a web site (or a link to another web site) for the customer who obtains an insurance product or service electronically and agrees to receive the notice at the web site.
- G. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.
- H. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 5.A., 6.A. and 9.A., respectively, by providing one notice to those consumers jointly.

Section 12 Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties

- A. Conditions for disclosure.
 1. Except as otherwise authorized in this regulation, a licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless:
 - a. The licensee has provided to the consumer an initial notice as required under Section 5;
 - b. The licensee has provided to the consumer an opt out notice as required in Section 8;
 - c. The licensee has given the consumer a reasonable opportunity, before it discloses the information to the nonaffiliated third party, to opt out of the disclosure; and
 - d. The consumer does not opt out.
 2. Opt out definition. Opt out means a direction by the consumer that the licensee not disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as permitted by Sections 15, 16 and 17.

3. A licensee provides a consumer with a reasonable opportunity to opt out if:
 - a. The licensee mails the notices required in Section 12.A.1. to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within thirty (30) days from the date the licensee mailed the notices.
 - b. A customer opens an on-line account with a licensee and agrees to receive the notices required in Section 12.A.1. electronically, and the licensee allows the customer to opt out by any reasonable means within thirty (30) days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.
 - c. For an isolated transaction such as providing the consumer with an insurance quote, a licensee provides the consumer with a reasonable opportunity to opt out if the licensee provides the notices required in Section 12.A.1. at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.
- B. Application of opt out to all consumers and all nonpublic personal financial information.
 1. A licensee shall comply with this section, regardless of whether the licensee and the consumer have established a customer relationship.
 2. Unless a licensee complies with this section, the licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer that the licensee has collected, regardless of whether the licensee collected it before or after receiving the direction to opt out from the consumer.
- C. A licensee may allow a consumer to select certain nonpublic personal financial information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.

Section 13 Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information

- A. Information the licensee receives under an exception.
 1. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution under an exception in Sections 16 or 17 of this regulation, the licensee's disclosure and use of that information is limited as follows:
 - a. The licensee may disclose the information to the affiliates of the financial institution from which the licensee received the information;
 - b. The licensee may disclose the information to its affiliates, but the licensee's affiliates may, in turn, disclose and use the information only to the extent that the licensee may disclose and use the information; and
 - c. The licensee may disclose and use the information pursuant to an exception in Sections 16 or 17 of this regulation, in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

2. Example. If a licensee receives information from a nonaffiliated financial institution for claims settlement purposes, the licensee may disclose the information for fraud prevention, or in response to a properly authorized subpoena. The licensee may not disclose that information to a third party for marketing purposes or use that information for its own marketing purposes.
- B. Information a licensee receives outside of an exception.
1. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution other than under an exception in Sections 16 or 17 of this regulation, the licensee may disclose the information only:
 - a. To the affiliates of the financial institution from which the licensee received the information;
 - b. To its affiliates, but its affiliates may, in turn, disclose the information only to the extent that the licensee may disclose the information; and
 - c. To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which the licensee received the information.
 2. Example. If a licensee obtains a customer list from a nonaffiliated financial institution outside of the exceptions in Sections 16 or 17:
 - a. The licensee may use that list for its own purposes; and
 - b. The licensee may disclose that list to another nonaffiliated third party only if the financial institution from which the licensee purchased the list could have lawfully disclosed the list to that third party. That is, the licensee may disclose the list in accordance with the privacy policy of the financial institution from which the licensee received the list, as limited by the opt out direction of each consumer whose nonpublic personal financial information the licensee intends to disclose, and the licensee may disclose the list in accordance with an exception in Sections 16 or 17, such as to the licensee's attorneys or accountants.
- C. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under an exception in Sections 16 or 17 of this regulation, the third party may disclose and use that information only as follows:
1. The third party may disclose the information to the licensee's affiliates;
 2. The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and
 3. The third party may disclose and use the information pursuant to an exception in Sections 16 or 17 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.
- D. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party other than under an exception in Sections 16 or 17 of this regulation, the third party may disclose the information only:
1. To the licensee's affiliates;

2. To the third party's affiliates, but the third party's affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and
3. To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

Section 14 Limits on Sharing Account Number Information for Marketing Purposes

- A. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.
- B. Section 14.A. of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:
 1. To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;
 2. To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or
 3. To a participant in an affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.
- C. Examples.
 1. A policy number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as the licensee does not provide the recipient with a means to decode the number or code.
 2. For the purposes of this section, a policy or transaction account is an account other than a deposit account or a credit card account. A policy or transaction account does not include an account to which third parties cannot initiate charges.

Section 15 Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Service Providers and Joint Marketing

- A. General rule.
 1. The opt out requirements in Sections 8 and 12 do not apply when a licensee provides nonpublic personal financial information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:
 - a. Provides the initial notice in accordance with Section 5; and
 - b. Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 16 or 17 in the ordinary course of business to carry out those purposes.

2. Example. If a licensee discloses nonpublic personal financial information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Section 15.A.1.b. if it prohibits the institution from disclosing or using the nonpublic personal financial information except as necessary to carry out the joint marketing or under an exception in Sections 16 or 17 in the ordinary course of business to carry out that joint marketing.
- B. The services a nonaffiliated third party performs for a licensee under Section 15.A. may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.
- C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 16 Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions

- A. The requirements for initial notice in Section 5.A.2., the opt out in Sections 8 and 12, and service providers and joint marketing in Section 15 do not apply if the licensee discloses nonpublic personal financial information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:
 1. Servicing or processing an insurance product or service that a consumer requests or authorizes;
 2. Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;
 3. A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or
 4. Reinsurance or stop loss or excess loss insurance.
- B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:
 1. Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or
 2. Required, or is a usual, appropriate or acceptable method:
 - a. To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;
 - b. To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;
 - c. To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

- d. To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;
- e. To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or
- f. In connection with:
 - (1) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;
 - (2) The transfer of receivables, accounts or interests therein; or
 - (3) The audit of debit, credit or other payment information.

Section 17 Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information

- A. The requirements for initial notice to consumers in Section 5.A.2., the opt out in Sections 8 and 12, and service providers and joint marketing in Section 15 do not apply when a licensee discloses nonpublic personal financial information:
 - 1. With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;
 - 2. For licensee and consumer protection.
 - a. To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;
 - b. To protect against or prevent actual or potential fraud or unauthorized transactions;
 - c. For required institutional risk control or for resolving consumer disputes or inquiries;
 - d. To persons holding a legal or beneficial interest relating to the consumer; or
 - e. To persons acting in a fiduciary or representative capacity on behalf of the consumer;
 - 3. To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

4. To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;
 5. To a consumer reporting agency.
 - a. To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or
 - b. From a consumer report reported by a consumer reporting agency;
 6. In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal financial information concerns solely consumers of the business or unit;
 7. For compliance purposes.
 - a. To comply with federal, state or local laws, rules and other applicable legal requirements;
 - b. To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or
 - c. To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or
 8. For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.
- B. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 8.F.
- C. Licensees placed into receivership or liquidation are exempt from the notice requirements in this Regulation. During the receivership or liquidation the licensee shall not disclose any nonpublic personal information about its customers or former customers except as permitted by law.

Section 18 When Authorization is Required for Disclosure of Nonpublic Personal Health Information

- A. A licensee shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

- B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity, underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers' compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods, to enforce licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.

Section 19 Authorizations

- A. A valid authorization to disclose nonpublic personal health information pursuant to Sections 18 through 22 shall be in written or electronic form and shall contain all of the following:
1. The identity of the consumer or customer who is the subject of the nonpublic personal health information;
 2. A general description of the types of nonpublic personal health information to be disclosed;
 3. General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure, and how the information will be used;
 4. The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and
 5. Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.
- B. An authorization for the purposes of Sections 18 through 22 shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.
- C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to Sections 18 through 22 at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.
- D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

Section 20 Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt out notice pursuant to Section 11., provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or customer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 18.A.

Section 21 Application of Federal Statutes and Regulations

Application of federal regulations concerning privacy of personal health information.

- A. Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services, "Standards for the Privacy of Individually Identifiable Health Information," if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of Sections 18 through 22.
- B. Nothing in this regulation is intended to require a carrier that is not subject the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services, "Standards for the Privacy of Individually Identifiable Health Information" to comply with the federal regulation.

Section 22 Relationship to Colorado Laws

Nothing in this regulation shall preempt or supersede existing Colorado law related to medical records, health or insurance information privacy.

Section 23 Protection of Fair Credit Reporting Act

Nothing in this regulation shall be construed to modify, limit or supersede the operation of the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be drawn on the basis of the provisions of this regulation regarding whether information is transaction or experience information under Section 603 of that Act.

Section 24 Nondiscrimination

- A. A licensee shall not unfairly discriminate against any consumer or customer because that consumer or customer has opted out from the disclosure of his or her nonpublic personal financial information pursuant to the provisions of this regulation.
- B. A licensee shall not unfairly discriminate against a consumer or customer because that consumer or customer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this regulation.

Section 25 Incorporation by Reference

The federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), published by the Government Publishing Office shall mean the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), as published on the effective date of this regulation and does not include later amendments to or editions of the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.). A copy of the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) may be examined during regular business hours at the Colorado Division of Insurance, 1560 Broadway, Suite 850, Denver, Colorado 80202. A certified copy of the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) may be requested from the Colorado Division of Insurance for a fee. A copy may also be obtained online at www.uscode.house.gov.

The Bank Holding Company Act of 1956 (12 U.S.C. 1841, et seq.) published by the Government Publishing Office shall mean The Bank Holding Company Act of 1956 (12 U.S.C. 1841, et seq.), as published on the effective date of this regulation and does not include later amendments to or editions of The Bank Holding Company Act of 1956 (12 U.S.C. 1841, et seq.). A copy of The Bank Holding Company Act of 1956 (12 U.S.C. 1841, et seq.) may be examined during regular business hours at the Colorado Division of Insurance, 1560 Broadway, Suite 850, Denver, Colorado 80202. A certified copy of The Bank Holding Company Act of 1956 (12 U.S.C. 1841 et seq.) may be requested from the Colorado Division of Insurance for a fee. A copy may also be obtained online at www.uscode.house.gov.

The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.) published by the Government Publishing Office shall mean The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), as published on the effective date of this regulation and does not include later amendments to or editions of The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.). A copy of The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.) may be examined during regular business hours at the Colorado Division of Insurance, 1560 Broadway, Suite 850, Denver, Colorado 80202. A certified copy of The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.) may be requested from the Colorado Division of Insurance for a fee. A copy may also be obtained online at www.uscode.house.gov.

Section 26 Severability

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

Section 27 Enforcement

Noncompliance with this regulation may result in the imposition of any of the 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 revocation of license, subject to the requirements of due process.

Section 28 Effective Date

- A. This regulation is effective January 14, 2018. In order to provide sufficient time for licensees to establish policies and procedures to comply with the requirements of this regulation, the commissioner will not pursue enforcement of these provisions prior to April 1, 2018.
- B. By April 1, 2018, a licensee shall provide an initial notice, as required by Section 5, to consumers who are the licensee's customers on or before April 1, 2018. If the licensee will not disclose any nonpublic personal financial information about the customer to any nonaffiliated third party, such initial notice may be delayed until the earlier of the renewal date of the policy or April 1, 2019.

Section 29 History

Emergency Regulation 00-E-1, effective September 5, 2000.
New Regulation 6-4-1, effective December 1, 2000.
Amended Regulation, effective July 1, 2001.
Amended Regulation effective January 14, 2018.

APPENDIX A – Sample Clauses

The safe harbor of compliance for use of these sample clauses expires on July 1, 2019.

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1: Categories of information a licensee collects (all institutions)

A licensee may use this clause, as applicable, to meet the requirement of Section 7.A.1. to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us, our affiliates or others; and
- Information we receive from a consumer reporting agency.

A-2: Categories of information a licensee discloses (institutions that disclose outside of the exceptions)

A licensee may use one of these clauses, as applicable, to meet the requirement of Section 7.A.2. to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections 15, 16 and 17.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

- Information we receive from you on applications or other forms, such as [provide illustrative examples, such as “your name, address, social security number, assets, income, and beneficiaries”];
- Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as “your policy coverage, premiums, and payment history”]; and
- Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as “your creditworthiness and credit history”].

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as “above” or “below”].

A-3: Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions)

A licensee may use this clause, as applicable, to meet the requirements of Sections 7.A. 2., 3., and 4. to describe the categories of nonpublic personal information about customers and former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal financial information to any party, other than as permitted by the exceptions in Sections 16 and 17.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A-4: Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)

A licensee may use this clause, as applicable, to meet the requirement of Section 7.A.3. to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 15, 16 and 17, as well as when permitted by the exceptions in Sections 16 and 17.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

- Financial service providers, such as [provide illustrative examples, such as “life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents”];
- Non-financial companies, such as [provide illustrative examples, such as “retailers, direct marketers, airlines, and publishers”]; and
- Others, such as [provide illustrative examples, such as “non-profit organizations”].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A-5: Service provider/joint marketing exception

A licensee may use one of these clauses, as applicable, to meet the requirements of Section 7.A.5. related to the exception for service providers and joint marketers in Section 15. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

- Information we receive from you on applications or other forms, such as [provide illustrative examples, such as “your name, address, social security number, assets, income, and beneficiaries”];

- Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as “your policy coverage, premium, and payment history”]; and
- Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as “your creditworthiness and credit history”].

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as “above” or “below”] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A-6: Explanation of opt out right (institutions that disclose outside of the exceptions)

A licensee may use this clause, as applicable, to meet the requirement of Section 7.A.6. to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 15, 16 and 17.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as “call the following toll-free number: (insert number)].

A-7: Confidentiality and security (all institutions)

A licensee may use this clause, as applicable, to meet the requirement of Section 7.A.8. to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as “those employees who need to know that information to provide products or services to you”]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

- (a) The Model Form may be used, at the option of a “licensee”), including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt out notice set forth in Colorado Insurance Regulation 6-4-1.
- (b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.
- (c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.
- (d) The word “customer” may be replaced by the word “member,” whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two (2) pages, which may be printed on both sides of a single sheet of paper or may appear on two (2) separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction Section B.3.a.i., or provides additional information in accordance with Instruction Section B.3.c. and such list or additional information exceeds the space available on page two of the Model Form, such list or additional information may extend to a third page.

- (a) Page One. The first page consists of the following components:
 - (1) Date last revised (upper right-hand corner);
 - (2) Title;
 - (3) Key frame (Why? What? How?);
 - (4) Disclosure table (“Reasons we can share your personal information”);

- (5) "To limit our sharing" box, as needed, for the licensee's opt out information;
 - (6) "Questions" box, for customer service contact information; and
 - (7) Mail-in opt out form, as needed.
- (b) Page Two. The second page consists of the following components:
- (1) Heading (Page 2);
 - (2) Frequently Asked Questions ("Who we are" and "What we do");
 - (3) Definitions; and
 - (4) "Other important information" box, as needed.

3. The Format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

- (a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.
- (b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.
- (c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.
- (d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.
- (e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

- 1. Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever name of licensee appears.
- 2. Page One:

- (a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as “rev. [month/year]” using either the name or number of the month, such as “rev. July 2016” or “rev. 7/16.”
- (b) General instructions for the “What?” box.
 - (i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term “Social Security number” in the first bullet.
 - (ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.
- (c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Section B.2.d. of this Instruction. In the middle column, each licensee must provide a “Yes” or “No” response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

“Yes,” if it is required to or voluntarily provides an opt out; “No,” if it does not provide an opt out; or

“We don’t share,” if it answers “No” in the middle column.

Only the sixth row (“For our affiliates to market to you”) may be omitted at the option of the licensee. See Section B.2.d.vi. of this Instruction.
- (d) Specific disclosures and corresponding legal provisions.
 - (i) For our everyday business purposes. This reason incorporates sharing information under [Sections 16 and 17 of Colorado Insurance Regulation 6-4-1 and with service providers pursuant to Colorado Insurance Regulation 6-4-1] other than the disclosures described in Section B.2.d.ii. or Section B.2.d.iii. of this Instruction.
 - (ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to Colorado Insurance Regulation 6-4-1. A licensee that shares for this reason may choose to provide an opt out.

- (iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between two (2) or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [Section 15 of Colorado Insurance Regulation 6-4-1. A licensee that shares for this reason may choose to provide an opt out.
- (iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt out.
- (v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt out.
- (vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt out; or the licensee provides the affiliate marketing notice separately. Licensees that include this reason must provide an opt out of indefinite duration. A licensee that is required to provide an affiliate marketing opt out, but does not include that opt out in the Model Form under this part, must comply with section 624 of the FCRA and Colorado Insurance Regulation 6-4-1, with respect to the initial notice and opt out and any subsequent renewal notice and opt out. A licensee not required to provide an opt out under this subparagraph may elect to include this reason in the Model Form.
- (vii) For nonaffiliates to market to you. This reason incorporates sharing described in Sections 8 and 12.A. of Colorado Insurance Regulation 6-4-1. A licensee that shares personal information for this reason must provide an opt out.
- (e) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt out page or a general web address that provides a clear and conspicuous direct link to the opt out page. The opt out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt out information are in Section B.2.g.v. of these Instructions.

- (f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words “toll-free” before the telephone number, as appropriate.
- (g) Mail-in opt out form. Licensees must include this mail-in form only if they state in the “To limit our sharing” box that consumers can opt out by mail. The mail-in form must provide opt out options that correspond accurately to the “Yes” responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as “[account #].” Licensees that require additional or different information, such as a random opt out number or a truncated account number to implement an opt out election should modify the “[account #]” reference accordingly. This includes licensees that require customers with multiple accounts to identify each account to which the opt out should apply. A licensee must enter its opt out mailing address in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt out form must not include any content of the model form.
- (i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with Section B.3.a.5. of these Instructions, must include in the far left column of the mail-in form the following statement:
- If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.
- ☐ Apply my choice(s) only to me.
- The word “choice” may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word “policy” for “account” in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.
- (ii) FCRA Section 603(d)(2)(A)(iii) opt out. If the licensee shares personal information pursuant to Section 603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt out form the following statement:
- ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.
- (iii) FCRA Section 624 opt out. If the licensee uses Section 624 of the FCRA, in accord with Section B.2.d.6. of these Instructions, it must include in the mail-in opt out form the following statement:
- ☐ Do not allow your affiliates to use my personal information to market to me.
- (iv) Nonaffiliate opt out. If the licensee shares personal information pursuant to Section 12.A. of Colorado Insurance Regulation 6-4-1, it must include in the mail-in opt out form the following statement:

☐ Do not share my personal information with nonaffiliates to market their products and services to me.

- (v) Additional opt outs. Licensees that use the disclosure table to provide opt out options beyond those required by federal law must provide those opt outs in this section of the Model Form. A licensee that chooses to offer an opt out for its own marketing in the mail-in opt out form must include one of the two following statements:

☐ Do not share my personal information to market to me; or

☐ Do not use my personal information to market to me.

A licensee that chooses to offer an opt out for joint marketing must include the following statement:

☐ Do not share my personal information with other financial institutions to jointly market to me.

- (h) Barcodes. A licensee may elect to include a barcode and/or “tagline” (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

- (a) General Instructions for the Questions. Certain questions on the Model Form may be customized as follows:

- (i) “Who is providing this notice?” This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two (2) or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by Section 11.F. Colorado Insurance Regulation 6-4-1. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the “Other important information” box, or, if that box is not included in the licensee’s form, directly following the “Definitions.” The list may appear in a multi-column format.
- (ii) “How does [name of licensee] protect my personal information?” The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the licensee’s use of cookies or other measures it uses to safeguard personal information. Licensees are limited to a maximum of thirty (30) additional words.

- (iii) “How does [name of licensee] collect my personal information?”
Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver’s license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: “We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.” Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: “We also collect your personal information from other companies.” Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

- (iv) “Why can’t I limit all sharing?” Licensees that describe state privacy law provisions in the “Other important information” box must use the bracketed sentence: “See below for more on your rights under state law.” Other licensees must omit this sentence.
- (v) “What happens when I limit sharing for an account I hold jointly with someone else?” Only licensees that provide opt out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: “Your choices will apply to everyone on your account.” Or “Your choices will apply to everyone on your account—unless you tell us otherwise.” Licensees may substitute the word “policy” for “account” in these statements.

- (b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three (3) definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

- (i) Affiliates. As required by Section 7.A.3. of Colorado Insurance Regulation 6-4-1, where [affiliate information] appears, the licensee must:

- (a) If it has no affiliates, state: “[name of licensee] has no affiliates”;

- (b) If it has affiliates but does not share personal information with them, state: “[name of licensee] does not share with our affiliates”; or
 - (c) If it shares with its affiliates, state, as applicable: “Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list].”
- (ii) Nonaffiliates. As required by Section 7.C.3. of Colorado Insurance Regulation 6-4-1], where [nonaffiliate information] appears, the licensee must:
 - (a) If it does not share with nonaffiliated third parties, state: “[name of licensee] does not share with nonaffiliates so they can market to you”; or
 - (b) If it shares with nonaffiliated third parties, state, as applicable: “Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations].”
- (iii) Joint Marketing. As required by Section 15. of Colorado Insurance Regulation 6-4-1, where [joint marketing] appears, the licensee must:
 - (a) If it does not engage in joint marketing, state: “[name of licensee] doesn’t jointly market”; or
 - (b) If it shares personal information for joint marketing, state, as applicable: “Our joint marketing partners include [list categories of companies such as credit card companies].”
- (c) General instructions for the “Other important information” box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:
 - (i) State and/or international privacy law information; and/or
 - (ii) A form by which the consumer may acknowledge receipt of the notice.

Regulation 6-4-2 STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Section 1	Authority
Section 2	Scope and Purpose
Section 3	Applicability
Section 4	Definitions
Section 5	Information Security Program
Section 6	Objectives of Information Security Program
Section 7	Examples of Methods of Development and Implementation
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(1), and 10-16-109, C.R.S.

Section 2 Scope and Purpose

- A. This regulation establishes standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, pursuant to Sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807.
- B. Section 501(a) provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) requires the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical and physical safeguards:
 - 1. To ensure the security and confidentiality of customer records and information;
 - 2. To protect against any anticipated threats or hazards to the security or integrity of such records; and
 - 3. To protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.
- C. Section 505(b)(2) calls on state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by regulation with respect to persons engaged in providing insurance.
- D. Section 507 provides, among other things, that a state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. This regulation requires that the safeguards established pursuant to this regulation shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

Section 3 Applicability

This regulation applies to all licensees operating in the state of Colorado.

A licensee domiciled in Colorado that is in compliance with this regulation in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in such other state.

Section 4 Definitions

- A. "Customer" means, for the purpose of this regulation, a consumer who has a customer relationship with a licensee.
- B. "Customer information" means, for the purpose of this regulation, nonpublic personal financial information and nonpublic personal health information about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.
- C. "Customer information systems" means, for the purpose of this regulation, the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.
- D. "Health information" means, for the purpose of this regulation, any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:
 - 1. The past, present or future physical, mental or behavioral health or condition of an individual;
 - 2. The provision of health care to an individual; or
 - 3. Payment for the provision of health care to an individual.
- E. "Licensee" means, for the purpose of this regulation, all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized pursuant to the insurance laws of Colorado, except that "licensee" shall not include: a purchasing group or a nonadmitted insurer in regard to the surplus lines business conducted pursuant to Title 10, Article 5, C.R.S.
- F. "Nonpublic personal financial information" means, for the purpose of this regulation:
 - 1. Personally identifiable financial information; and
 - 2. Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
 - 3. Nonpublic personal financial information does not include:
 - a. Health information;
 - b. Publicly available information
 - c. Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.
 - 4. Examples of lists.

- a. Nonpublic personal financial information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.
 - b. Nonpublic personal financial information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.
- G. "Nonpublic personal health information" means, for the purpose of this regulation, health information:
 - 1. That identifies an individual who is the subject of the information; or
 - 2. With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.
- H. "Service provider" means, for the purpose of this regulation, a person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

Section 5 Information Security Program

Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Section 6 Objectives of Information Security Program

A licensee's information security program shall be designed to:

- A. Ensure the security and confidentiality of customer information;
- B. Protect against any anticipated threats or hazards to the security or integrity of the information; and
- C. Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Section 7 Examples of Methods of Development and Implementation

The actions and procedures described in this section are examples of methods of implementation of the requirements of Sections 5 and 6 of this regulation. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement Sections 5 and 6 of this regulation.

- A. Assess Risk. The licensee:
 - 1. Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and
 3. Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.
- B. Manage and Control Risk. The licensee:
1. Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;
 2. Trains staff, as appropriate, to implement the licensee's information security program; and
 3. Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.
- C. Oversee Service Provider Arrangements. The licensee:
1. Exercises appropriate due diligence in selecting its service providers; and
 2. Requires its service providers to implement appropriate measures designed to meet the objectives of this regulation and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.
- D. Adjust the Program

The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

Section 8 Severability

If any provision of this regulation or 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 of the 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 revocation of license, subject to the requirements of due process.

Section 10 Effective Date

This amended regulation shall become effective on January 14, 2018.

Section 11 History

New Regulation 6-4-2 effective November 1, 2002.

Amended regulation effective January 14, 2018.

Regulation 6-5-1 CONCERNING THE REPORTING OF SUSPECTED INSURANCE FRAUD

Section 1	Authority
Section 2	Scope and Purpose
Section 3	Applicability
Section 4	Definitions
Section 5	Rules
Section 6	Severability
Section 7	Enforcement
Section 8	Effective Date
Section 9	History

Section 1 Authority

This regulation is promulgated and adopted by the Commissioner of Insurance under the authority of § § 10-1-109 and 10-4-1003 C.R.S.

Section 2 Scope and Purpose

The purpose of this regulation is to facilitate the reporting of suspected insurance fraud, to aid in the detection, investigation and ultimate prosecution of those who commit insurance fraud in this state and to deter future fraudulent acts by improving regulatory oversight of licensed persons who commit insurance fraud.

This regulation describes the procedure and circumstances under which all insurers shall, and individuals may, report suspected insurance fraud for the purpose of investigating, and enforcing laws prohibiting insurance fraud.

Section 3 Applicability

This regulation applies to all insurers, nonprofit hospital, medical-surgical, and health service corporations, health maintenance organizations, licensed insurance producers and other persons or corporations that are required or elect to report insurance fraud in the state of Colorado.

Section 4 Definitions

- A. "Authorized agency" shall have the same meaning as provided in § 10-4-1002(1), C.R.S.
- B. "Concealment" means the knowing concealment of a material fact by impeding the discovery of the material fact, by misrepresentation or by willful omission.

- C. "Fraudulent insurance act" includes an act done by a person, with intent to defraud, in presenting, causing to be presented, or prepares with the knowledge or belief that it will be presented, to or by an insurer, a purported insurer, a producer, or any representative thereof; a written statement as part, or in support of, an application for the issuance or the rating of an insurance policy or a claim for payment or other benefit pursuant to an insurance policy that he or she knows to contain false information concerning any fact material thereto; any act done by a person, knowingly and with intent to defraud or mislead conceals information concerning any fact or circumstance material thereto; or any act described as a criminal offense in Titles 8, 10, 12, and 18, C.R.S., regarding the provision or acquisition of any policy of insurance, the misappropriation of any payment of premium or benefit, the presentation of payment of claim or insurance benefit, or any other matter.
- D. "Insurer" means every person engaged as principal, indemnitor, surety, or contractor in the business of making contracts of insurance and every insurer and any person licensed or regulated under Title 10, C.R.S. and Pinnacol Assurance.
- E. "Intentionally" or "with intent". A person acts intentionally or with intent with the person's conscious objective is to cause the specific result proscribed by a statute defining an offense, or a rule or regulation requiring or prohibiting a particular action. It is immaterial to the issue of intent whether or not the result actually occurred.
- F. "Material fact". A fact is material if a reasonable person under the circumstances would attach importance to it in making a decision or determining a course of action, including but not limited to the issuance of a policy, the payment or acceptance of premiums, the submission of a claim, the scope or direction of an investigation, whether a claim should be paid or not, or the amount to be paid on a claim or benefit to any party.
- G. "Medical record" means the written or graphic documentation, sound recording, or computer record of services pertaining to medical and health care which are performed at the direction of a physician or other licensed health care provider on behalf of a patient by physicians, dentists, nurses, technicians, emergency medical technicians, pre-hospital providers or other healthcare personnel. Medical record includes such diagnostic documentations as x-rays, electrocardiograms, electroencephalograms, and other test results.
- H. "Misrepresentation" means any oral or written communication or conduct, or combination of communication and conduct that is untrue and is intended to create a misleading impression in the mind of another.
- I. "NAIC Online Fraud Reporting System" means the online, consumer accessible reporting system hosted by the National Association of Insurance Commissioners and located at <https://eapps.naic.org/ofrs/ofrsHome.jsp>
- J. "Notice" or "notify" means the notification, in writing to an Authorized agency or a Secondary Agency by any person or insurer.
- K. "Person" means every natural person, firm, partnership, association, or corporation, or other business entity or trust, except insurers.
- L. "Policy" means an individual or group policy, group certificate, contract or arrangement of insurance or reinsurance affecting the rights of a resident of this state or bearing a reasonable relation to this state, regardless of whether delivered or issued for delivery in this state.
- M. "Relevant" means any information having a tendency to make the existence of any fact that is of consequence to the investigation or determination or the issue more probable or less probable than it would be without the information or evidence.

- N. "Secondary Agency" shall have the same meaning as provided in § 10-4-1002(6), C.R.S. Secondary Agencies shall include, but not be limited to, the National Insurance Crime Bureau (NICB), the National Association of Insurance Commissioners (NAIC) and the National Health Care Anti-Fraud Association (NHCAA).

Section 5 Rules

Reporting Requirements

A. Reporting Required

1. Each insurer licensed to do business in this state that obtains a judgment or settlement in a lawsuit involving a fraudulent insurance act against a person who is licensed by the state of Colorado and whose services are compensated in whole or in part, directly or indirectly, by insurance claim proceeds, shall send to the appropriate Colorado state licensing board and the Colorado Division of Insurance, notice of such settlement.
2. Every person who obtains a judgment or settlement involving a fraudulent insurance act by an insurer or a representative of an insurer may send to the Colorado Division of Insurance notice of such judgment or settlement, including any evidence of a fraudulent insurance act.
3. When any person or insurer has reason to believe that a fire loss might have been caused by other than accidental means or that any insurance claim may be fraudulent, then such person may, and such insurer shall, notify an authorized agency or Secondary Agency; except that if such fire loss or insurance claim has been caused by a licensed insurance producer or insurer then the notifying person may and the notifying insurer shall notify the Colorado Division of Insurance.
4. When any person or insurer has reason to believe that any claim for insurance benefits or policy application is in whole or in part a fraudulent insurance act or contains a material misrepresentation or concealment of a material fact, then such person may, and such insurer shall, notify an authorized agency or Secondary Agency; except that if such fraudulent insurance act, material misrepresentation or concealment of a material fact has been committed by a licensed insurance producer or insurer then the notifying person may and the notifying insurer shall notify the Colorado Division of Insurance.
5. Nothing in paragraphs A.1. through A.4. of this section 5 shall preclude a person or an insurer from reporting to more than one authorized agency, Secondary Agency, or combination of authorized and Secondary agencies.

B. Minimum Information, Suggested Format for Reporting and Timelines for Reporting

1. All notifications provided to the Colorado Division of Insurance should be made using the NAIC Online Fraud Reporting System. If the NAIC OnLine Fraud Reporting System is not utilized then the following information must be provided:
 - a. The name, address and telephone number of the reporting party and the name and telephone number of a contact person;
 - b. When available, the name, address, physical description, and telephone number of any suspect, and any identifying information such as date of birth, social security number, tax identification number, drivers license number, aliases, and vehicle identification number if an automobile is involved;

- c. The location of the incident;
- d. A detailed description of the claimed injury, if applicable.
- e. A synopsis of the facts of the fraudulent insurance act, misrepresentation or concealment; and
- f. A list of any other authorized agencies or secondary agencies to which the activity or claim has been reported, if applicable.

Notification, when not made using the NAIC Online Fraud Reporting System, shall, whenever practical, be made through electronic mail to DORA_INS_Fraudreporting@state.co.us.

- 2. All notifications to an authorized agency other than the Colorado Division of Insurance and all notifications to a Secondary Agency shall be reported in the format, if any, required or requested by such agency.
- 3. A person may report a suspected insurance fraud at any time.
- 4. An insurer shall report the fraudulent insurance act no later than sixty (60) days after the date its investigation is completed and facts are sufficient to establish a reasonable suspicion that a reportable act has occurred, or within sixty (60) days of the receipt of a judgment or settlement.

C. Release of information

- 1. A notification to an authorized agency shall be confidential, shall not constitute a public record under part 2 of article 72 of title 24, C.R.S., shall not be subject to subpoena, and shall not be discoverable or admissible in any civil action, except that any authorized agency provided with relevant information or evidence pursuant to this subsection one (1), or subsection two (2) below, may release such information to any other authorized agency, which shall hold the information confidential, except as is set forth at § 10-4-1004, C.R.S.
- 2. This regulation shall not be construed to prohibit the admission of evidence of a fraudulent insurance act in any civil litigation involving such insurance act. This regulation shall also not be construed to prohibit the admission of evidence of a fraudulent insurance act in any civil litigation that involves the alleged confidential disclosure of information by an insurer or person if that insurer or person does not meet the criteria for immunity set forth at § 10-4-1005, C.R.S.
- 3. No insurer or authorized agency shall intentionally refuse to release non-proprietary or non-private information concerning a possible non-accidental fire loss or fraudulent insurance act, upon request, to an insurer that is or could be required to pay a claim to which such information relates or to any other authorized agency.
- 4. Any authorized agency may, in writing, require the insurer having an interest in a claim to release to the authorized agency or other insurer specific, relevant, non-proprietary or non-private information or evidence which the insurer has in its possession and which relates to a claim. Relevant information may include, but shall not be limited to:
 - a. Insurance policy information pertaining to a claim under investigation and any application for such policy;

- b. Policy premium payment records;
 - c. History of previous claims made by the insured;
 - d. Any other non-privileged or non-private material relating to the investigation of the loss, including statements of any person who may have information about the loss, and any proof of such loss;
 - e. Photographs, audio or video recordings made pursuant to the investigation;
 - f. Medical records, if the release is permitted or require by law without an authorization, or the authorized agency has an authorization for the procurement and release of those records;
 - g. Examinations under oath, if any; and
 - h. Chronology, if available.
5. Any insurer providing information to an authorized agency or agencies pursuant to this regulation may, in writing, request such agency to release to such insurer specific, relevant information or evidence relating to the fire loss or other claim under investigation. Such agency may, in its sole discretion, and with such restrictions as such agency deems appropriate, release such information to such insurer.
6. Any insurer providing information pursuant to this section shall cooperate with any law enforcement agency of competent jurisdiction and other insurers.
7. Any request for the release of information hereunder shall be solely for the purpose of detecting, investigating, preventing or prosecuting an actual or suspected fraudulent insurance act. Information so provided shall not be used for underwriting or rating purposes except in connection with an application or policy under which a fraudulent insurance act was committed. Information released pursuant to such request shall be subject to the confidentiality and immunity provisions of § § 10-4-1003 and 10-4-1005, C.R.S., and shall not be a public record under part 2 of article 72 of title 24, C.R.S., and shall not be discoverable or admissible in any civil action.
8. No waiver of any applicable privilege or claim of confidentiality in the documents, materials or information shall occur as a result of disclosure to the Colorado Division of Insurance under this section or as a result of sharing the information with another insurer or Secondary Agency pursuant to this regulation or § § 10-4-1003 or 10-4-1005, C.R.S.
9. The Colorado Division of Insurance or Secondary Agency shall promptly notify the insurer in the event that documents submitted by the insurer or Secondary Agency pursuant to this regulation are subpoenaed. Such notification shall include a copy of the subpoena and be made in the most expeditious practical method available to the Colorado Division of Insurance or the Secondary Agency. The Colorado Division of Insurance or Secondary Agency shall make a good faith effort to give the notification to the person or to the department of the insurer, which furnished the documents being subpoenaed.

Section 6 Enforcement

Noncompliance with this regulation may result in the imposition of any of the 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 revocation of license, subject to the requirements of due process.

Section 7 Severability

In the event any part of this regulation is determined to be invalid for any reason, the remainder of the regulation shall not be affected.

Section 8 Effective Date

This regulation shall become effective on November 1, 2013.

Section 9 History

Original regulation effective May 1, 2003
Regulation repealed and repromulgated in full effective July 1, 2012
Amended Regulation revised effective November 1, 2013

Editor's Notes

History

Regulation 6-2-1 repealed eff. 06/01/2012
Regulations 6-3-1, 6-5-1 eff. 07/01/2012.
Regulation 6-5-1 eff. 11/01/2013.
Regulation 6-1-1 eff. 10/15/2015.
Regulation 6-3-2 eff. 02/01/2016.
Regulations 6-4-1, 6-4-2 eff. 01/14/2018.
Regulation 6-3-1 eff. 06/01/2018.