Issue Brief #3

HJR 21 - Study of Personal Information Ownership

For the State Administration and Veterans' Affairs Interim Committee
Prepared by Sheri Scurr, Research Analyst
Montana Legislative Services Division

April 19, 2016

Financial Services Providers: Current Law Exceptions Allowing for the Disclosure of Personal Information

Purpose and Scope

This issue brief responds to the State Administration and Veterans' Affairs Interim Committee's Feb. 10, 2016, request for further research about the exceptions in Montana's current law covering insurance companies that allows personal information to be disclosed for certain purposes and under certain circumstances.

This brief covers:

- Montana's current law.
- Federal law.
- Other states' laws.

Montana's Current Law

The Montana Insurance Information and Privacy Protection Act was enacted in 1981 and is administered by the State Auditor's Office.

Under the act, certain insurance businesses are prohibited from sharing a customer's personal information, except as specified in the act. In other words, personal information may be disclosed only for specified purposes and only under specified circumstances.

In all cases, a customer's personal information may be shared only with the written authorization of the customer (i.e., by an "opt-in" affirmative consent).

Who is covered?

A licensee is defined as:

> "an insurance institution, insurance producer, or other person who is licensed or required to be licensed, authorized or required to be authorized, or registered or required to be registered pursuant to this title; or ... a surplus lines insurer." (Section 33-19-104(16), MCA)

What is covered?

Personal information is defined as:

> "any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information includes an individual's name and address and medical record information but does not include privileged information."
> (Section 33-19-104(21), MCA)

Privileged information is defined as:

> "any individually identifiable information that:
>
> (a) relates to a civil or criminal proceeding involving an individual; and
>
> (b) is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving an individual. Information otherwise meeting the requirements of privileged information under this subsection is considered personal information under this chapter if it is disclosed in violation of 33-19-306."
> (Section 33-19-104(24), MCA)

What are the exceptions?

As previously noted, under Montana's law, personal information may not be shared except as specifically authorized in one of two statutes, either section 33-19-306, MCA, for non-marketing purposes, or section 33-19-307, MCA, for marketing purposes.

The term "disclosure" is used in both of these sections to mean the sharing of personal information, rather than as a reference to disclosing a privacy policy to the individual.

Sharing personal information for non-marketing purposes

Section 33-19-306, MCA, was originally enacted in 1981. Most of the subsections require that the information sharing must be reasonably necessary for the specified purpose and that the entity receiving the information may not use the information for any other purpose or further share the information without the customer's written consent.

Under the section, disclosure may be made to the following types of entities for the following purposes:

- to another person for:
  - detecting or preventing criminal activity, fraud, material misrepresentation, or material nondisclosure in connection with an insurance transaction.

- to another licensee for:
  - detecting or preventing criminal activity, fraud, material misrepresentation, or material nondisclosure in connection with insurance transactions; or
  - performing an insurance function.

- to a medical care institution, a medical professional, or the individual to whom the information pertains for:
  - verifying insurance coverage or benefits;
  - informing an individual of a medical problem of which the individual may not be aware;
  - conducting an operations or services audit; or
  - determining the reasonableness or necessity of medical services.

- to an insurance regulatory authority.

- to a law enforcement or other government authority or to an insurance regulatory agency:
    - for protecting the interests of a licensee in preventing, investigating, or prosecuting the perpetration of fraud upon a licensee;
    - because of a reasonable belief that illegal activities have been conducted by the individual; or
    - for the online motor vehicle liability insurance verification system.

- to an actuarial or research entity for conducting actuarial or research studies if:
    - an individual is not identified in any actuarial or research report;
    - materials allowing the individual to be identified are returned or destroyed as soon as they are no longer needed.

- to a licensee's affiliate for:
    - use of the information in connection with an audit of the licensee;
    - a licensee to perform an insurance function; or
    - marketing, as allowed by 33-19-307.

- to a group policyholder if "reasonably necessary" for:
    - reporting claims experience or conducting an audit of the licensee's operations or services. But, medical record information disclosed must be edited to prevent the identification of the applicant, policyholder, or certificate holder.

- to a party or a representative of a party to a proposed sale, transfer, merger, or consolidation of all or part of the business of the licensee or insurance-support organization if "reasonably necessary" for:
    - the information recipient to make business decisions about the purchase, transfer, merger, or consolidation is disclosed; and

- to a lienholder, mortgagee, assignee, lessor, or other person shown on the records of an insurance institution or insurance producer as having a legal interest in a policy of insurance if "reasonably necessary" for:
    - the person's interests in that policy.

- to a professional peer review organization for:
    - the purpose of reviewing the service or conduct of a medical care institution or medical professional.

- to a governmental authority:
    - as required by federal or state law; or
    - for the purpose of determining the individual's eligibility for health benefits for which the governmental authority may be liable.

- to a certificate holder or policyholder for:
    - providing information regarding the status of an insurance transaction. Disclosure may not be made to a group policyholder without a separate, written authorization from the individual.

- to a person contractually engaged to provide services:
    - to enable a licensee to perform an insurance function; or
    - to enable the contractor to perform an insurance function on behalf of a licensee.

- 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 if:
    - the disclosure is limited to that which is reasonably necessary to enable the person or entity to perform services or an insurance function for the disclosing licensee; and
    - the person or entity is notified by the licensee that the person or entity is prohibited from using the information, other than to carry out the limited purpose for which the information is disclosed.

Disclosure does not have to be "reasonably necessary" if the disclosure is for:

- health research that is subject to the approval of an institutional review board and the requirements of federal law and regulations governing biomedical research;

- epidemiological or drug therapy outcomes research that requires information that has been made anonymous to protect the identity of the patient through coding or encryption.

The MCA section includes the following "catch all" authorization:

- If a licensee has to disclose personal or privileged information in order to perform an insurance function and disclosure is not permitted under another exception in this section, disclosure may be made to a person other than a licensee if:

- the disclosure is limited to that which is reasonably necessary to enable the person to perform services or an insurance function for the disclosing licensee; and
- the person receiving the information is notified by the licensee that the person is prohibited from:
    - using the information other than to carry out the limited purpose for which the information is disclosed; and
    - disclosing the information other than to the licensee and as allowed in the subsection.

Sharing personal information for marketing purposes

Section 33-19-307, MCA, which was enacted in 2001, prohibits the sharing of personal information for marketing purposes, except as outlined in the section. Under the section, disclosure may occur only for the purpose of marketing financial or insurance products and services and only to the following entities:

- Another licensee.

- An affiliate, which is a person/organization who "directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with another person/organization.

- A person who is contractually engaged to provide marketing services for the licensee.

In general, any disclosure must be "reasonably necessary" and may not include medical record information. Furthermore, the entity receiving the information may not use the information for any other purpose than for marketing financial products and services.

Additionally, disclosure may only occur with the written consent of the individual and only if the consent form meets all of the following criteria:

- Clearly and conspicuously states that the disclosed information is intended to be used for marketing purposes.

- Specifies each entity or type of entity to which the licensee intends to disclose the information.

- Specifies what information the licensee intends to disclose.

- Specifies the type of marketing that the individual might receive pursuant to the disclosure.

Authorization Form

Montana's law also specifies the content of the disclosure authorization form by which the customer is to provide consent. Section 33-19-206, MCA, provides the following:

- A valid authorization to disclose personal information must be in written form, or in electronic form as provided by applicable law, and must contain the following:

  (a) the identity of the individual who is the subject of the personal information;

  (b) a description of the types of personal information to be disclosed;

  (c) a description of the entity or type of entity to which the licensee discloses personal information, the purpose of the disclosure, and how the information will be used;

  (d) the signature of the individual who is the subject of the personal information or the individual who may by law allow the disclosure and the date on which the authorization is signed; and

  (e) notice of the length of time for which the authorization is valid, notice that the individual may revoke the authorization at any time, and notice of the procedure for revocation.

- An authorization remains valid for a period stated in the authorization that does not exceed 24 contiguous months.

- An individual who is the subject of personal information and has signed an authorization may revoke the authorization at any time.

- A licensee shall retain the original authorization or a copy of it in the record of the individual who is the subject of personal information.

- A licensee may not condition enrollment, coverage, benefits, or rates on an individual's signing of a disclosure authorization unless the disclosure sought through the authorization is necessary for the licensee to perform an insurance function.

Federal Law

The Financial Services Modernization Act (Gramm-Leach-Baily Act (GLBA)) (15 U.S.C. 6801 through 6827) is the primary privacy law governing the financial industry. The law was originally enacted in 1999, more than 17 years after Montana's Insurance Information and Privacy Protection Act, but a few years before Montana's code section authorizing disclosure of personal information for marketing purposes.

The FTC's regulation implementing the Act is called the Financial Privacy Rule.

Overall Framework

In contrast to Montana's approach of prohibiting the sharing of information, except as authorized by the state statute, the GLBA requires covered entities to notify consumers of their information practices and then allow the consumers to opt out.

Who is covered?

The federal law is also broader than Montana's law in terms of the institutions covered. The GLBA covers any business engaged in financial activities, not just insurance companies (there are a few narrow exceptions).

What information is covered?

The GLBA covers all nonpublic personal information (NPI), which is any personally identifiable financial information that a financial institution collects or obtains about an individual in connection with providing a financial product or service and that is not otherwise publicly available.

The FTC's website provides a summary of the GLBA provisions. The website states that NPI is information that is not otherwise publically available and that is as follows:

- Any information given in order to get a financial product or service (for example, name, address, income, Social Security number, or other information on an application).

- Any information obtained about an individual from a transaction involving an individual's financial product(s) or service(s) (for example, the fact that an individual is a customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases).

- Any information obtained by the financial institution when investigating the individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

Source: FTC website
https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

---

THE FOLLOWING INFORMATION IS AN EXTRACT OF THE FTC INFORMATION ON THE GLBA - WITH EMPHASIS ADDED BY STAFF

Opt-Out Notices

General Obligations

If you share their NPI **with nonaffiliated third parties** outside of three exceptions (see "Exceptions"), you must give your consumers and customers an "opt-out notice" that clearly and conspicuously describes their right to opt out of the information being shared. An opt-out notice must be delivered with a privacy notice, and it can be part of the privacy notice.

The opt-out notice must describe a "reasonable means" for consumers and customers to opt out. They must receive the notice and have a reasonable opportunity to opt out before you can disclose their NPI to these nonaffiliated third parties. Acceptable "reasonable means" to opt out include a toll-free telephone number or a detachable form with a check-off box and mailing information. Requiring the consumer or customer to write a letter as the only option is not a "reasonable means" to opt out.

Note: While the GLB Act does not require you to provide an opt-out notice if you only disclose NPI to affiliates, if you share certain information

with your affiliates, you may have an obligation to provide an opt-out notice under the Fair Credit Reporting Act. That opt-out notice must be included in your GLB privacy notice (see "Fair Credit Reporting Act").

Exercising the Opt-Out Right

You must give consumers and customers a "reasonable opportunity" to exercise their right to opt out, for example, 30 days, after you send the initial notice either on- or off-line, before you can share their information with nonaffiliated third parties outside the exceptions. For an isolated consumer transaction, like buying a money order, you may require your consumers to make their opt-out decision before completing the transaction.

Consumers and customers who have the right to opt out may do so at any time. Once you receive an opt-out direction from your existing consumers or customers, you must comply with it as soon as is reasonably possible.

The Shelf Life of an Opt-Out Direction

An opt-out direction by a consumer or customer is effective - even after the customer relationship is terminated - until canceled in writing, or, if the consumer agrees, electronically. However, if a former customer establishes a new customer relationship with you and you are required to provide an opt-out notice, the customer must make a new opt-out direction that will apply only to the new relationship.

SUMMARY OF NOTICE REQUIREMENTS

Initial Customers. Not later than when you establish the customer relationship, unless it would substantially delay the transaction and the customer agrees Description of information-collection and sharing practices, and opt-out notice (if you share NPI with nonaffiliated third parties outside of certain exceptions)

Consumers who are not customers. (including former customers) Before you disclose their NPI to a nonaffiliated third party outside of certain exceptions Full description of information-collection and sharing practices or "short-form" notice, along with opt-out notice

Annual Customers. Delivery on a consistent basis at least once in any period of 12 consecutive months for the duration of the customer relationship Description of information-collection and sharing practices, and opt-out notice (if you share NPI with nonaffiliated third parties outside of certain exceptions)

Exceptions

Exceptions to the Notice and Opt-Out Requirements

There are a number of exceptions to the notice and opt-out requirements. These exceptions are located in sections 313.14 ("section 14 exceptions") and 313.15 ("section 15 exceptions") of the Privacy Rule. If you share information only under these sets of exceptions, you don't need to give your consumers a privacy notice, but you will need to give your customers a simplified initial and, if applicable, an annual privacy notice. Customers and consumers have no right to opt out of these disclosures of NPI.

The section 14 exceptions apply to various **types of information-sharing that are necessary for processing or administering a financial transaction requested or authorized by a consumer.** This includes, for example, disclosing NPI to service providers who help mail account statements and perform other administrative activities for a consumer's account. It also includes disclosures to and by creditors listed by a consumer on a credit application to perform a credit check.

The section 15 exceptions apply to certain **types of information-sharing, including disclosures for purposes of preventing fraud, responding to judicial process or a subpoena, or complying with federal, state, or local laws.** Examples of appropriate information disclosures under this exception include those made to technical service providers who maintain the security of your records; your attorneys or auditors; a purchaser of a portfolio of consumer loans you own; and a consumer reporting agency, consistent with the Fair Credit Reporting Act (see "Exceptions").

Exception to the Opt-Out Requirement: Service Providers and Joint Marketing

Another exception can be found in section 313.13 ("section 13 exception") of the Privacy Rule. If you share information under this exception, you must give your customers - and your consumers if you share their information - a privacy notice that describes this disclosure. However, your consumers and customers do not have a right to opt out of this information sharing.

The section 13 exception covers **disclosures for certain service providers and for certain marketing activities**. The section 13 exception covers disclosures to **third party service providers** whose services for you do not fall within the section 14 exceptions. For example, if you hire a nonaffiliated third party to provide services in connection with marketing your products or to market financial products jointly for you and another financial institution, or to do a general analysis of your customer transactions, your disclosure of NPI for these purposes does not fall under the section 14 exceptions. Therefore, you can use the section 13 exception for these types of service providers.

The section 13 exception **also applies to marketing financial products or services offered through a "joint agreement"** with one or more other financial institutions. The "joint agreement" requirement means that you have entered into a written contract with one or more financial institutions about your joint offering, endorsement, or sponsorship of a financial product or service. This does not apply to any kind of joint marketing you do, but only joint marketing with other financial institutions and only the marketing of financial products or services.

To take advantage of the section 13 exception, you must enter into a contract with those nonaffiliated third parties with whom you share NPI. The agreement must guarantee the confidentiality of the information by prohibiting the third party or parties from using or disclosing the information for any purpose other than the one for which it was received. Contracts with nonaffiliated service providers that are effective before July 1, 2000 and don't have the required confidentiality agreement must be amended to include such a provision by July 1, 2002

END OF EXTRACT FROM FTC WEBSITE

Other States

California

Financial Information Privacy Act, California - Financial Code sections 4050 - 4060.

- Prohibits financial institutions from sharing or selling personally identifiable nonpublic information without obtaining a consumer's consent, as provided.
- Requires a plain-language notice of the privacy rights it confers.
- Requires that a consumer must "opt in" before a financial institution may share personal information with an unaffiliated third party.
- Requires that consumers be given an opportunity to "opt out" of sharing with a financial institution's financial marketing partners.
- Requires that consumers be given the opportunity to "opt out" of sharing with a financial institution's affiliates, with some exceptions. When an affiliate is wholly owned, in the same line of business, subject to the same functional regulator and operates under the same brand name, an institution may share its customers' personal information with the affiliate without providing an opt-out right.

Source: California Office of Attorney General Privacy Laws web page https://oag.ca.gov/privacy/privacy-laws

[More Research To Do]