MICROFILM DIVIDER

OMB/RECORDS MANAGEMENT DIVISION
SFN 2053 (2/85) 5M

ROLL NUMBER

DESCRIPTION

2127

2001 SENATE INDUSTRY, BUSINESS AND LABOR

SB 2127

2001 SENATE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB 2127

Senate Industry, Business and Labor Committee

❑ Conference Committee

Hearing Date January 30, 2001.

Tape Number	Side A	Side B	Meter #
1		x	15.8 to end
2	x		6.5 to 31.2
Committee Clerk Signature	Doris E Perez		

Minutes:

The meeting was called to order. All committee members present. Hearing was opened on SB 2127 relating to the insurance commissioner sharing confidential information with other state agencies.

Jim Poolman, Insurance Commissioner, in favor of the bill. Written testimony attached, including copy of Privacy of Consumer Financial and Health Information Regulation and of PCFHIR Frequently Asked Questions. I firmly believe consumers need protection of their financial and medical information and from marketing to third party affiliates. Present laws do not address the regulation of insurance companies privacy activities. This bill gives the insurance commissioner that authority. We will address opt-in/opt-out rights of consumers regarding medical and financial information. Medical information should have more restrictive standards (opt-in to allow disclosure), that is why I favor this bill.

Senator Tollefson : Page 3 of the rules prohibit disclosure of "nonpublic" information, what

would be "public information"?

J Poolman: Public: anything you put in an application, like phone number in insurance policy app.. Nonpublic: medical diagnosis.

Senator Klein NCOIL Model Act is less restrictive than NAIC's?

J Poolman: Yes, especially the opt-out standard for medical information is less restrictive than the opt-in we support here today.

Leah Coghland, AIA: Submitted proposed amendment.

Senator Tollefson: Your amendment would propose opt-out.

J Poolman: This amendment would allow us to not become more restrictive than the NAIC Model Act: opt-out for financial information and opt-in for medical information. NCOIL : opt-out for both financial and medical information.

Senator Mathern: What is the meaning of the last sentence in the proposed amendment?

Leah Coghland: No one can come against the department for not enacting those regulations.

Chuck Johnson, Chief Legal Counsel ND Ins Dept. : Public in general does not have private cause of action to sue because of violation of privacy law. Under this law a private citizen cannot sue for money, the department can take administrative action.

Marilyn Foss, NDBA, : We support this bill as collolary to SB2191. Adopting GLB approach regarding private information makes things uniform at the national level for financial institutions.

Dan Ulmer, Blue Cross/ Blue Shield: Background information: HIPA allowed portability, creating the issue of how to measure outcome/quality, have to look at data, how do we unify data and privacy? From the insurers perspective it makes more sense to institute things at the federal level, easier because most of us are doing business in other states. Since the HIPA bill, Congress was supposed to act on what these rules were going to look like; they demurred on HHS which

promulgated rules last December. Now we are basically trying to comply: first to put together data for uniformity, and with the privacy rules on how can we share information electronically and on paper. We have to be compliant with HIPA by 7/01/02. We are trying to be compliant with HIPA and GLB. We have a problem with which one to comply, we think we are HIPA so I am offering an amendment to exempt us from GLB until 8/01/03.

Rod St Aubyn, BC/BS, Regulations say if you are HIPA compliant you are exempt from GLB.

Senator Espegard: Is HIPA more stringent than GLB?

J Poolman: Yes, our goal is not to provide more regulations, we believe HIPA probably is more stringent than our particular privacy rules.

Chuck Johnson: If you are not planning to market information, you don't have to worry about compliance. We disagree with the blues on the implementation date.

J Poolman: I don't think they should be exempted, if you comply with HIPA, you comply with us, so I don't think they should be exempted.

Recess. Committee reconvened. All members present.

J Poolman: We reached an agreement, scrap the Blues amendment exempting them from regulations. We think we can address their concerns with the HIPA regulations vs. GLB regulations, and who would be deemed in compliance with those particular regulations, in the rule making process. If Blues were working towards compliance with HIPA privacy rules we can potentially deem them in compliance or exempt based on our discussions during the rulemaking process, if you folks see that as fair. I want this as part of the record in legislative intent so we can make clear with the Blues that the conversation has taken place and we can go forward in the rulemaking process, provided the bill passes, and we can address that at that point in time. By then we will have a clear picture, hopefully, of what is going to actually happen with HIPA rules,

considering we have a new President and new Secretary of HHS. By then we can have a better grasp of where we are all going to be towards the end of the year when we get into the rules making process that the insurance department will have to get through to promulgate the rules with this particular bill.

Senator Every: What we are doing is what they asked but not putting it in the bill?

J Poolman: No, by addressing it in the rulemaking process we still keep them as part of privacy rule, but by then we would have a clear idea of how GLB privacy rules and HIPA rules actually coordinate. We don't know that now but we don't want to give up the potential consumer protections for the people of ND by putting that in state law. We don't want duplication that would confuse the consumer either. We will address the effective date in the rulemaking process. We struck a deal that allows department to protect consumer and satisfy the Blues so they don't have to incur extra expenses. We want to adopt the NAIC standard of opt-in for medical information and opt-out for financial information, this will provide us with uniformity around the country.

Dan Ulmer, BC/BS: this is what we really wanted to establish. So many questions are unanswered as this unfurls.

Brenda Blazer, IAA: To clarify: exception with GLB as long as comply with HIPA applies to all insurance companies.

Senator Klein: What is the status now? Banks have opt out standard and insurance companies require written authorization?

D Ulmer: The industry practice is that when you sign up for insurance you sign release for exchange of information for claims processing, not for information to be sold.

Senator Klein: Motion to adopt AIA amendment **Senator Espegard**: Second.

Roll call vote: 6 yes; 1 no. Motion carried.

Senator Espegard: Motion: do pass as amended. **Senator Krebsbach**: Seconded.

Roll call vote: 6 yes; 1 no. Motion carried. Floor assignment: **Senator Klein**.

Date: 1/30/01
Roll Call Vote #: 1

2001 SENATE STANDING COMMITTEE ROLL CALL VOTES
BILL/RESOLUTION NO. 2127

Senate Senate Industry, Business and Labor Committee

☐ Subcommittee on _____
or
☐ Conference Committee

Legislative Council Amendment Number _____

Action Taken A I A amendments adoption

Motion Made By Sen Klein Seconded By S Espegard

Senators	Yes	No	Senators	Yes	No
Senator Mutch - Chairman	✓		Senator Every	✓	
Senator Klein - Vice Chairman	✓		Senator Mathern	✓	
Senator Espegard	✓				
Senator Krebsbach	✓				
Senator Tollefson		✓			

Total (Yes) 6 No 1

Absent _____

Floor Assignment _____

If the vote is on an amendment, briefly indicate intent:

Date: 1/30/01
Roll Call Vote #: 2

2001 SENATE STANDING COMMITTEE ROLL CALL VOTES
BILL/RESOLUTION NO. 2127

Senate Senate Industry, Business and Labor Committee

☐ Subcommittee on _____
or
☐ Conference Committee

Legislative Council Amendment Number _____

Action Taken DPA

Motion Made By Sen Espegaard Seconded By Sen Krebsbach

Senators	Yes	No	Senators	Yes	No
Senator Mutch - Chairman	✓		Senator Every	✓	
Senator Klein - Vice Chairman	✓		Senator Mathern	✓	
Senator Espegard	✓				
Senator Krebsbach	✓				
Senator Tollefson		✓			

Total (Yes) 6 No 1

Absent _____

Floor Assignment Sen Klein

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

SB 2127: Industry, Business and Labor Committee (Sen. Mutch, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (6 YEAS, 1 NAY, 0 ABSENT AND NOT VOTING). SB 2127 was placed on the Sixth order on the calendar.

Page 1, line 12, after the underscored period insert "The rules must be consistent with and not more restrictive than the model regulation adopted by the national association of insurance commissioners entitled "Privacy of Consumer Financial and Health Information Regulation". This section does not create a private right of action."

Renumber accordingly

2001 HOUSE INDUSTRY, BUSINESS AND LABOR

SB 2127

2001 HOUSE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB 2127

House Industry, Business and Labor Committee

☐ Conference Committee

Hearing Date March 7, 2001

Tape Number	Side A	Side B	Meter #
1		X	15.5-41.3
Committee Clerk Signature			

Minutes: Chairman R. Berg, Vice-Chair G. Keiser, Rep. M. Ekstrom, Rep. R. Froelich, Rep. G. Froseth, Rep. R. Jensen, Rep. N. Johnson, Rep. J. Kasper, Rep. M. Klein, Rep. Koppang, Rep. D. Lemieux, Rep. B. Pietsch, Rep. D. Ruby, Rep. D. Severson, Rep. E. Thorpe.

Jim Poolman: *ND Insurance Commissioner* **Written testimony.**

Rep Froseth: What is "right of action"?

Poolman: That is an AIA amendment dealing with privacy.

Vice-Chairman Keiser: Could an insuring bank review check stubs?

Poolman: That could still happen now.

Dan Ulmer: *BC/BS* HIPA makes insurance portable. From job to job and tries to uniform and privatize nationally. Everyone needs to be compliant by 7/1/02. GLB is the other regulator and the two clash. We would like to exempt companies that have to be HIPA compliant. HIPA is opt-in.

Pat Ward: *ND Domestic Insurance Co.'s* We support this bill.

Gary Thune: We also support this bill.

Jack McDonald: *Individual Community Banks of ND* We support this bill.

Marilyn Foss: *NDBA* We support this bill as well.

Poolman: If a company is in compliance with us, you are in compliance with HIPA.

Chairman Berg: We'll close the hearing on SB 2127.

2001 HOUSE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB 2127

House Industry, Business and Labor Committee

☐ Conference Committee

Hearing Date March 7, 2001

Tape Number	Side A	Side B	Meter #
3	X		17.1-21.0
Committee Clerk Signature			

Minutes: Chairman R. Berg, Vice-Chair G. Keiser, Rep. M. Ekstrom, Rep. R. Froelich, Rep. G. Froseth, Rep. R. Jensen, Rep. N. Johnson, Rep. J. Kasper, Rep. M. Klein, Rep. Koppang, Rep. D. Lemieux, Rep. B. Pietsch, Rep. D. Ruby, Rep. D. Severson, Rep. E. Thorpe.

Jim Poolman: *ND Insurance Commissioner* If you are in compliance with HIPA you will be in compliance with our rules, working to become in compliance is the same. GLB sets the minimum standards for finance, HIPA is for medical.

Vice-Chairman Keiser: I move a do pass.

Rep M. Klein: I second.

15 yea, 0 nay, 0 absent Carrier Rep Froseth

Date: 3-7-01
Roll Call Vote #: 1

2001 HOUSE STANDING COMMITTEE ROLL CALL VOTES
BILL/RESOLUTION NO. SB 2127

House Industry, Business and Labor Committee

Legislative Council Amendment Number

Action Taken Do Pass

Motion Made By Keiser Seconded By M. Klein

Representatives	Yes	No	Representatives	Yes	No
Chairman- Rick Berg	✓		Rep. Jim Kasper	✓	
Vice-Chairman George Keiser	✓		Rep. Matthew M. Klein	✓	
Rep. Mary Ekstorm	✓		Rep. Myron Koppang	✓	
Rep. Rod Froelich	✓		Rep. Doug Lemieux	✓	
Rep. Glen Froseth	✓		Rep. Bill Pietsch	✓	
Rep. Roxanne Jensen	✓		Rep. Dan Ruby	✓	
Rep. Nancy Johnson	✓		Rep. Dale C. Severson	✓	
			Rep. Elwood Thorpe	✓	

Total (Yes) 15 No 0

Absent 0

Floor Assignment Rep Froseth

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE (410)
March 7, 2001 3:48 p.m.

Module No: HR-38-5050
Carrier: Froseth
Insert LC: . Title: .

REPORT OF STANDING COMMITTEE

SB 2127: Industry, Business and Labor Committee (Rep. Berg, Chairman) recommends **DO PASS** (15 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2127 was placed on the Fourteenth order on the calendar.

2001 TESTIMONY

SB 2127

SENATE BILL NO. 2127

Presented by: **Jim Poolman**
Commissioner
North Dakota Insurance Department

Before: **Industry, Business and Labor Committee**
Senator Duane Mutch, Chairman

Date: **January 30, 2001**

TESTIMONY

Mr. Chairman and members of the committee:

Good Morning. My name is Jim Poolman and I am the Commissioner of Insurance for the State of North Dakota. I appear here in support of SB 2127, the Insurance Department's privacy bill.

Section 1

Section 1 of SB 2127 provides that insurance companies, nonprofit health service corporations, or health maintenance organizations may not disclose nonpublic personal information contrary to the provisions of Title V of the Gramm-Leach-Bliley Act (GLBA).

GLBA, also known as the Financial Modernization Act, allows banks, insurance companies, credit unions, thrift associations, securities firms, investment companies, and other businesses to enter into each other's markets and to become affiliates within a financial holding company.

Title V of GLBA outlines the privacy restrictions under which a financial institution must operate. It reads, "It is the policy of 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' non-public personal information."

Privacy became a concern after it was discovered that, without the consumer's consent or knowledge, certain banks were selling customer credit card information to non-affiliated marketing firms. The activity was discovered when bank customers noticed unauthorized charges appearing on their credit card billings.

GLBA defines a "financial institution" such that the definition includes an insurance company. Unlike the activities of banks, thrift institutions, and securities firms that are subject to federal agency regulation, state regulators regulate insurance company activities. A state regulator, however, receives the authority to regulate from the state legislature. Our present laws do not specifically address the regulation of insurance company privacy activities. This bill gives the State Insurance Commissioner that authority.

Financial Information

Title V first requires that a financial institution develop a privacy policy. Before disclosing non-public personal information to a non-affiliated third party, the financial institution must inform a consumer of that policy and give the consumer the opportunity to direct that the information not be disclosed to non-affiliated third parties. This is known as giving the consumer the right to "opt out". Thus, if the consumer "opt-outs", a financial institution cannot disclose the consumer's non-public personal financial information to a non-affiliated third party.

GLBA allows a financial institution to disclose non-public personal information to certain third parties without the consumer's consent under certain circumstances, including:

- The sharing of non-public personal financial information with its affiliates.
- The sharing of non-public personal financial information with third parties that perform services for or functions on behalf of the financial institution.
- The sharing of non-public personal financial information with third parties engaged in a joint marketing activity with the financial institution.

Thus, GLBA allows affiliates to share non-public personal information with one another and does not allow a consumer to prevent the sharing of information among affiliates.

Medical Information

GLBA deals specifically with a consumer's non-public **personal** information. Personal information includes that information collected by a financial institution from a consumer. Because insurance companies are financial institutions and because insurance companies collect medical information, the term "personal information" includes medical information. GLBA's privacy provisions do not distinguish between a personal **financial** information and a personal **medical** information.

State insurance regulators agreed that medical information deserves greater privacy protections than those given to personal financial information. State insurance regulators are concerned that an insurance company could share a customer's sensitive personal medical information with a third party, whether an affiliate or not, to the consumer's detriment. For example, a customer's home mortgage application could be denied if the mortgagee company found out about a customer's physical or mental health condition from an affiliated insurance company.

Although GLBA did not specifically address health information, the state insurance regulators developed certain rules relating to the disclosure of non-public personal medical information. Those rules prohibit an insurance company from disclosing non-public personal medical information to any third party unless the consumer specifically authorizes the disclosure.

This is known as requiring that the consumer "opt in" to allowing the disclosure. Thus, a customer must "opt-in" before an insurance company can disclose non-public personal medical information to either affiliated or non-affiliated third parties.

It should be noted that the customer's permission is not required if the disclosure is to third parties for legitimate business purposes, such as for claims processing, underwriting,

reinsurance, fraud investigation, and others.

To facilitate the Commissioner's enforcement of GLBA's privacy provisions, SB 2127 allows the Commissioner to develop rules. As Commissioner, I propose to adopt rules based on the proposed rules developed by the various state insurance regulators. A copy of those rules is attached as Appendix A. The rules adopt an "opt out" standard for the disclosure of non-public personal **financial** information to a non-affiliated third party, except for disclosures related to legitimate business purposes, and an "opt in" standard for the disclosure of non-public personal **medical** information, even to affiliates.

State insurance regulators such as myself are encouraging all states to adopt the state regulator's recommended privacy regulations so that there will be uniformity throughout the states. Numerous insurance companies operate throughout the United States. Uniformity among the states will enable the insurance industry to comply with all state regulations by developing a single set of privacy procedures.

Some insurance companies are recommending that states adopt regulations developed by the National Council of Insurance Legislators (NCOIL). I am familiar with those proposed regulations but believe that the state regulators proposed regulations provide stronger protections for a consumer's private medical information. For example, the NCOIL proposed regulations allow non-public personal medical information to be shared with a non-affiliated third party unless the consumer "opt outs". Our proposed regulations adopt an "opt in" standard for protecting non-public personal medical information.

Section 2

Section 2 of this bill allows the Commissioner to share confidential information, such as that discovered during our examinations of various insurance companies, with other agencies in this state. At present the law allows us to share such information with "state or federal regulatory or law enforcement officials from other states or jurisdictions" provided the officials are required, under their law, to maintain its confidentiality. The present law does not appear to allow us to share that same information with an agency in this state.

Section 2 will make this change.

I believe that sharing information with other agencies in this state, particularly with the Departments of Banking and Securities, is important because banks and securities and other financial institution firms are now allowed to engage in insurance activities. As each of the insurance, banking, thrift, and securities firms sell each other's products, it is important that the regulators be allowed to share information concerning their activities and their solvency with one another.

For your information, I have also attached a document entitled Privacy of Consumer and Financial and Health Information Model Regulations-Frequently Asked Questions that provides additional information concerning our proposed privacy regulations.

Requested Action

In light of the above, I am asking that the committee amend a "Do Pass" for SB 2127.

Thank you. I will be happy to try to answer any questions that you might have.

PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION REGULATION

Table of Contents

ARTICLE VI. ADDITIONAL PROVISIONS

ARTICLE I. GENERAL PROVISIONS

Section 1. Authority

This regulation is promulgated pursuant to the authority granted by Sections [insert applicable sections] of the Insurance Law.

Section 2. Purpose and Scope

A. Purpose. This regulation governs the treatment of nonpublic personal health information and nonpublic personal financial information about individuals by all licensees of the state insurance department. This regulation:

(1) Requires a licensee to provide notice to individuals about its privacy policies and practices;

(2) 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

(3) Provides methods for individuals to prevent a licensee from disclosing that information.

B. Scope. 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.

C. Compliance. A licensee domiciled in this state 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.

Drafting Note: Subsection C is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

Section 3. Rule of Construction

The examples in this regulation and the sample clauses in Appendix A of this regulation are not exclusive. Compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this regulation.

Section 4. Definitions

As used in this regulation, unless the context requires otherwise:

A. "Affiliate" means a company that controls, is controlled by or is under common control with another company.

B. (1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

(vi) Avoids explanations that are imprecise and readily subject to different interpretations.

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) 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.

(c) Notices on web sites. 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 ensure 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:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) 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.

C. "Collect" means 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.

D. "Commissioner" means the insurance commissioner of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

E. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

F. (1) "Consumer" means 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.

(2) Examples.

(a) 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.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) 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.

(d) An individual is a licensee's consumer if:

(i) (I) the individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) the individual is a claimant under an insurance policy issued by the licensee;

(III) the individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) the individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) the licensee discloses nonpublic personal financial information about the individual to a nonaffiliated third party other than as permitted under Sections 14, 15 and 16 of this regulation.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections 5, 6 and 9 of this regulation to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, workers' compensation plan participant, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about such an individual other than as permitted under Sections 14, 15 and 16 of this regulation, an individual is not the consumer of the licensee solely because he or she is:

(i) 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;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A beneficiary in a workers' compensation plan.

Drafting Note: Regulators may wish to urge their workers' compensation state insurance fund (or other applicable agency) to promulgate a regulation similar to this regulation in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be customers for purposes of this regulation.

(g) 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.

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

G. "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)).

H. "Control" means:

(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.

I. "Customer" means a consumer who has a customer relationship with a licensee.

J. (1) "Customer relationship" means 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.

(2) Examples.

(a) A consumer has a continuing relationship with a licensee if:

(i) The consumer is a current policyholder of an insurance product issued by or through the licensee; or

(ii) The consumer obtains financial, investment or economic advisory services relating to an insurance product or service from the licensee for a fee.

(b) A consumer does not have a continuing relationship with a licensee if:

(i) The consumer applies for insurance but does not purchase the insurance;

(ii) The licensee sells the consumer airline travel insurance in an isolated transaction;

(iii) The individual is no longer a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee;

(iv) 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;

(v) 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;

(vi) 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;

(vii) 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

(viii) 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.

K. (1) "Financial institution" means 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)).

(2) Financial institution does not include:

(a) 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.*);

(b) 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

(c) 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.

L. (1) "Financial product or service" means a 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)).

(2) 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.

M. "Health care" means:

(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.

N. "Health care provider" means 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.

O. "Health information" means 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.

P. (1) "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

(2) 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 a insurance product or service.

Q. (1) "Licensee" means 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 Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes, and cite appropriate state law.

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal financial information set forth in Articles I, II, III and IV 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.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal financial information set forth in Articles I, II, III and IV of this regulation provided:

(i) 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 14 of this regulation, except as permitted by Section 15 or 16 of this regulation; and

(ii) 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.

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

R. (1) "Nonaffiliated third party" means any person except:

(a) A licensee's affiliate; or

(b) 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).

(2) 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)).

S. "Nonpublic personal information" means nonpublic personal financial information and nonpublic personal health information.

T. (1) "Nonpublic personal financial information" means:

(a) Personally identifiable financial information; and

(b) 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.

(2) Nonpublic personal financial information does not include:

(a) Health information;

(b) Publicly available information, except as included on a list described in Subsection T(1)(b) of this section; 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.

(3) 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.

U. "Nonpublic personal health information" means 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.

V. (1) "Personally identifiable financial information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable financial information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) 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;

(iv) 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;

(v) 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;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable financial information does not include:

(i) Health information;

(ii) A list of names and addresses of customers of an entity that is not a financial institution; and

(iii) 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.

W. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public 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) Reasonable basis. 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) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. 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) Reasonable basis.

(i) 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.

(ii) 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.

ARTICLE II. PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION

Section 5. Initial Privacy Notice to Consumers Required

A. Initial notice requirement. A licensee shall provide a clear and conspicuous 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 Subsection 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 15 and 16.

B. When initial notice to a consumer is not required. A licensee is not required to provide an initial notice to a consumer under Subsection A(2) of this section 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 15 and 16, 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. When the licensee establishes a customer relationship.

(1) General rule. A licensee establishes a customer relationship at the time the licensee and the consumer enter into a continuing relationship.

(2) Examples of establishing customer relationship. A licensee establishes a customer relationship when the consumer:

(a) 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 insurance broker, obtains insurance through that licensee; or

(b) Agrees to obtain financial, economic or investment advisory services relating to insurance products or services for a fee from the licensee.

D. Existing customers. 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 Subsection A of this section 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 Subsection A of this section.

E. Exceptions to allow subsequent delivery of notice.

(1) A licensee may provide the initial notice required by Subsection 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) Not at customer's election. 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) Substantial delay of customer's transaction. 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) No substantial delay of customer's transaction. 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. Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 10. If the licensee uses a short-form initial notice for non-customers according to Section 7D, the licensee may deliver its privacy notice according to Section 7D(3).

Section 6. Annual Privacy Notice to Customers Required

A. (1) General rule. 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. (1) 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.

(2) Examples.

(a) 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.

(b) 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.

(c) 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.

(d) 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. Delivery. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 10.

Section 7. Information to be Included in Privacy Notices

A. General rule. 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 15 and 16;

(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 15 and 16;

(5) If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 14 (and no other exception in Sections 15 and 16 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 11A 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 Subsection B of this section.

B. Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under Sections 15 and 16, 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 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, as applicable:

(a) Information from the consumer;

(b) Information about the consumer's transactions with the licensee or its affiliates;

(c) Information about the consumer's transactions with nonaffiliated third parties; and

(d) 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 Paragraph (1), as applicable, and provides a few examples to illustrate the types of information in each category. These might include:

(i) Information from the consumer, including application information, such as assets and income and identifying information, such as name, address and social security number;

(ii) Transaction information, such as information about balances, payment history and parties to the transaction; and

(iii) 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 14 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 Subsection 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 Subsection A(2) of this section, as applicable; and

(b) States whether the third party is:

(i) A service provider that performs marketing services on the licensee's behalf or on behalf of the licensee and another financial institution; or

(ii) A financial institution with whom the licensee has a joint marketing agreement.

(5) Simplified notices. 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 15 and 16, the licensee may simply state that fact, in addition to the information it shall provide under Subsections A(1), A(8), A(9) and Subsection B of this section.

(6) Confidentiality and security. 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 5A(2) and 8C for a consumer who is not a customer by providing a short-form initial notice at the same time as 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 10. 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 10.

(4) Examples of obtaining privacy notice. 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. Future disclosures. The licensee's 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. Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this regulation.

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

A. (1) Form of opt out notice. If a licensee is required to provide an opt out notice under Section 11A, 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) Adequate opt out notice. 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:

(i) 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 7A(2) and (3), and states that the consumer can opt out of the disclosure of that information; and

(ii) 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) Reasonable opt out means. A licensee provides a reasonable means to exercise an opt out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt out notice;

(ii) Includes a reply form together with the opt out notice;

(iii) 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

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) Unreasonable opt out means. A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or

(ii) 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) Specific opt out means. A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. Same form as initial notice permitted. 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. Initial notice required when opt out notice delivered subsequent to initial notice. 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 Paragraph (5) of this subsection).

(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:

(i) It shall permit John and Mary to opt out for each other;

(ii) 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

(iii) 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. Time to comply with opt out. A licensee shall comply with a consumer's opt out direction as soon as reasonably practicable after the licensee receives it.

F. Continuing right to opt out. 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. Delivery. When a licensee is required to deliver an opt out notice by this section, the licensee shall deliver it according to Section 10.

Section 9. Revised Privacy Notices

A. General rule. 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 14, 15 and 16, 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. Delivery. When a licensee is required to deliver a revised privacy notice by this section, the licensee shall deliver it according to Section 10.

Section 10. Delivery

A. How to provide notices. 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. (1) Examples of reasonable expectation of actual notice. A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) 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;

(c) 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;

(d) 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.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not obtain an insurance product or service from the licensee electronically.

C. Annual notices only. 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.

D. Oral description of notice insufficient. A licensee may not provide any notice required by this regulation solely by orally explaining the notice, either in person or over the telephone.

E. Retention or accessibility of notices for customers.

(1) For customers only, a licensee shall provide the initial notice required by Section 5A(1), the annual notice required by Section 6A, 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) Examples of retention or accessibility. 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.

F. Joint notice with other financial institutions. 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.

G. Joint relationships. 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 5A, 6A and 9A, respectively, by providing one notice to those consumers jointly.

ARTICLE III. LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

Section 11. Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties

A. (1) Conditions for disclosure. 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 14, 15 and 16.

(3) Examples of reasonable opportunity to opt out. A licensee provides a consumer with a reasonable opportunity to opt out if:

(a) By mail. The licensee mails the notices required in Paragraph (1) of this subsection 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) By electronic means. A customer opens an on-line account with a licensee and agrees to receive the notices required in Paragraph (1) of this subsection 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) Isolated transaction with consumer. 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 Paragraph (1) of this subsection 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. Partial opt out. 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 12. Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information

A. (1) Information the licensee receives under an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution under an exception in Sections 15 or 16 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 15 or 16 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. (1) Information a licensee receives outside of an exception. If a licensee receives nonpublic personal financial information from a nonaffiliated financial institution other than under an exception in Sections 15 or 16 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 15 or 16:

(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 15 or 16, such as to the licensee's attorneys or accountants.

C. Information a licensee discloses under an exception. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under an exception in Sections 15 or 16 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 15 or 16 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. Information a licensee discloses outside of an exception. If a licensee discloses nonpublic personal financial information to a nonaffiliated third party other than under an exception in Sections 15 or 16 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 13. Limits on Sharing Account Number Information for Marketing Purposes

A. General prohibition on disclosure of account numbers. 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. Exceptions. Subsection 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) Policy number. 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) Policy or transaction account. 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.

ARTICLE IV. EXCEPTIONS TO LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

Section 14. 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 11 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 15 or 16 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 Paragraph (1)(b) of this subsection 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 15 or 16 in the ordinary course of business to carry out that joint marketing.

B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section 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 15. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section 5A(2), the opt out in Sections 8 and 11, and service providers and joint marketing in Section 14 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:

(i) 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;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

Section 16. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Financial Information

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 5A(2), the opt out in Sections 8 and 11, and service providers and joint marketing in Section 14 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) (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) (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) (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. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 8F.

Drafting Note: Because the notice requirements of this regulation could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this regulation.

ARTICLE V. RULES FOR HEALTH INFORMATION

Section 17. When Authorization 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 the 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 18. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article V 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 this Article V 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 this Article V 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 19. 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 10, 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 17A.

Section 20. Relationship to Federal Rules

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 [insert cite] (the "federal rule"), 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 this Article V.

Drafting Note: The drafters note that the effective date of this regulation is July 1, 2001. The HHS regulation is anticipated to be promulgated in late 2000, thereby becoming effective in late 2002. As of July 1, 2001, if the licensee is in compliance with all requirements of the HHS regulation except its effective date provision, the licensee is not subject to the provisions of this article. If the licensee comes into compliance with the HHS regulation after that date, the licensee is no longer subject to the provisions of this article as of the date the licensee comes into compliance with the HHS regulation.

Section 21. Relationship to State Laws

Nothing in this article shall preempt or supercede existing state law related to medical records, health or insurance information privacy.

ARTICLE VI. ADDITIONAL PROVISIONS

Section 22. 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 23. 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 24. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 25. Severability

If any section or portion of a section of this regulation or its applicability to any person or circumstance is held invalid by a court, the remainder of the regulation or the applicability of the provision to other persons or circumstances shall not be affected.

Section 26. Effective Date

A. Effective date. This regulation is effective November 13, 2000. In order to provide sufficient time for licensees to establish policies and systems to comply with the requirements of this regulation, the commissioner has extended the time for compliance with this regulation until July 1, 2001.

B. (1) Notice requirement for consumers who are the licensee's customers on the compliance date. By July 1, 2001, a licensee shall provide an initial notice, as required by Section 5, to consumers who are the licensee's customers on July 1, 2001.

(2) Example. A licensee provides an initial notice to consumers who are its customers on July 1, 2001, if, by that date, the licensee has established a system for providing an initial notice to all new customers and has mailed the initial notice to all the licensee's existing customers.

C. Two-year grandfathering of service agreements. Until July 1, 2002, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section 14A(1)(b) of this regulation, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before July 1, 2000.

APPENDIX A – SAMPLE CLAUSES

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 7A(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 7A(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 14, 15 and 16.

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 7A(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 information to any party, other than as permitted by the exceptions in Sections 15 and 16.

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 7A(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 14, 15 and 16, as well as when permitted by the exceptions in Sections 15 and 16.

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 7A(5) related to the exception for service providers and joint marketers in Section 14. 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 7A(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 14, 15 and 16.

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 7A(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.

Legislative History (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter (adopted).

Privacy of Consumer Financial and Health Information Model Regulation

Frequently Asked Questions

January 2001

FREQUENTLY ASKED QUESTIONS

PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION MODEL REGULATION

Table of Contents

Overview

The model regulation provides protection for financial and health information about consumers held by insurance companies, agents, and other entities engaged in insurance activities. In general, the model regulation requires insurers to:

1. Notify consumers about their privacy policies;

2. Give consumers the opportunity to prohibit the sharing of their protected financial information with nonaffiliated third parties; and

3. Obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates, and nonaffiliates alike.

The model regulation is now under consideration in the states. Some state insurance regulators may need to secure authorization from their state legislatures before they can promulgate the regulation; others may proceed without state legislative activity. Most states expect to have final privacy regulations promulgated by July 1, 2001.

Glossary of Terms

The following terms are used throughout this document:

"Affiliate" is a company that controls, is controlled by, or is under common control with another company. Under the Gramm-Leach-Bliley Act (GLBA), insurers and banks can become affiliates.

"Consumers" are individuals who are seeking to obtain, obtaining, or have obtained a product or service from an insurer. For example, an individual who has submitted an application for insurance is a consumer of the company to which he or she has applied, as is an individual whose policy with the company has expired.

"Customers" are consumers with whom insurers have on-going relationships. Policyholders are customers, for example.

"Insurers" are insurance companies, insurance agents, or other entities that are required to comply with the privacy regulation.

"Nonaffiliated third party" means a company that is not affiliated with an insurer.

"Opt in" means granting affirmative consent to the disclosure of protected information by an insurer. It only applies to health information. An insurer can share protected health information with other entities – including its affiliates or third parties – only if the customer or consumer opts in.

"Opt out" means prohibiting the disclosure of protected information by an insurer. It only applies to financial information. An individual can opt out of the disclosure of his or her protected financial information to third parties.

CONSUMER ISSUES

New Law Governing Insurers Protects Your Privacy

1. I understand there's a new law that lets banks, securities companies and insurance companies sell each other's products. What does this mean in terms of my own insurance coverage?

The new law, entitled the Gramm-Leach-Bliley Act (GLBA) after its congressional sponsors, breaks down the regulatory barriers between the banking, securities and insurance industries, allowing these types of companies to merge with each other and to engage in new business activities outside their traditional areas. Your insurance coverage should not be affected by the law, although your insurance company or agent might someday merge with a bank or expand its offerings to include banking products and services, such as loans, credit cards and mutual funds.

2. I just learned that my insurance company has changed to become a "financial holding company." What does this mean and how does it affect me?

This means that your insurance company is now permitted by law to start offering bank products such as loans, credit cards and mutual funds. It has either affiliated with an existing bank or is establishing a brand new bank. The bank division will actually be a separate company from the insurance company, but they will be related to each other within a larger holding company structure. Once they are affiliated, the companies are free to share all your personal financial information with each other without your permission.

3. Do I need to be worried that my own personal information is being shared or sold without my knowledge or permission by my insurance company or insurance agent?

Under the GLBA privacy provisions, your insurer cannot share your personal information without your knowledge, but they can disclose your information to certain parties without your permission.

Knowledge: GLBA and the model regulation require insurance companies, insurance agents, and other financial institutions such as banks to tell you about their policies for disclosing your personal financial information. Insurers are required to provide these privacy notices to you prior to disclosing any of your personal financial information.

Permission: Insurers are required to give you the opportunity to prohibit the sharing of certain financial information with unrelated companies, called "nonaffiliated third parties," but you may not prohibit the sharing of such information with your insurer's affiliates. In addition, you may not prohibit the disclosure of your personal information to third parties for things like claims processing, fraud investigations, and certain marketing efforts.

Importantly, the NAIC model privacy regulation also includes special protections for health information. The regulation requires insurance companies and agents to get your affirmative consent before sharing health information with any other entity.

4. Given the Internet and the information age, isn't this kind of personal information already public? Why are these new consumer privacy protection rules important? What do they mean for my family and me?

You are correct that there is a great deal of our personal information "out there" and these new privacy protections are important for that very reason. Financial institutions have ever-increasing amounts of information about their customers, and new technologies are enabling them to utilize this information in new and creative ways. With enactment of GLBA and the integration of banking, securities and insurance, there is concern that consumers could lose even more control over their personal information, and that this information could be used in ways in which consumers do not approve.

Of course, most companies value the trust and confidence of their customers, and treat personal information with respect. But even these companies might disclose your information in ways that you do not approve of – selling lists to marketers, for example.

For these reasons, Congress included consumer privacy protections in GLBA that set some basic standards that all financial institutions – including insurance companies and agents – must meet. These protections give you some control over the personal information that your financial institutions hold. In addition, by requiring financial institutions to tell you how they are going to disclose your information, Congress intended that you have enough information so that you can take your business elsewhere if you disagree with their disclosure policies.

The GLBA privacy provisions are embodied in regulations that will be issued by your state insurance commissioner. These regulations will govern how insurance companies and agents will protect your personal information in compliance with GLBA's privacy provisions. The NAIC has drafted a model regulation that will serve as the basis for the privacy regulations issued in most states.

5. How can an insurer access my personal financial and health information? Do they have to get it from me, or can they get the information through some other means?

Personal information protected under GLBA and the NAIC model regulation includes information that the company gets from you through your application, as well as information it collects as a result of your dealings with the company through transactions, submitting claims, etc. It also includes information the company gets from consumer reports and by tracking people who have used their Internet site.

6. What does this information have to do with my insurance policies?

Insurance companies hold this information because they need it to determine your insurance coverages and premiums and to pay your claims. The information could also be valuable to an insurer's ability to design and sell all sorts of products.

What Information is Protected under the New Law and Regulation?

7. Do these new protections apply to all my insurance policies - life, health, automobile, homeowners?

Generally, these protections apply to all types of insurance policies where the ultimate benefit goes to an individual (as opposed to a commercial entity). The following information is covered by these new protections:

- the information held by your car insurer;
- the information held by your homeowners insurer;
- the information held by your employer's group health plan;
- the information held by your life insurer;
- the information held by the insurer against which you made a claim related to a car accident;
- the information held by the life insurer for a life policy that names you as a beneficiary;
- the information held by your employer's workers' compensation insurer.

8. What information is protected by these privacy rules?

"Nonpublic personal financial information" and "nonpublic personal health information" are the general categories of information that are protected under the NAIC model regulation.

9. What does the term "non-public personal financial information" mean?

"Non-public personal financial information" is:

- information that you provide to your insurance company to obtain an insurance product or service (like income, credit history, name and address);

- information about you that the insurance company has as a result of a transaction with you involving an insurance product or service between the company and you (like premium payment history, how much your life insurance policy is worth, and the value of personal property insured); and

- all other information about you that the insurance company gets in connection with providing a product or service to you.

It also includes any list that is derived using such information. For example, a list that includes the names and income of an insurer's customers would be protected information.

Non-public personal information does not include publicly available information. Publicly available information is information that a company can get from a public source, such as a phone book, government records (including mortgage records), and the Internet.

10. What are some examples of my "non-public personal financial information"?

Examples of "non-public personal financial information" include:

- Information you provide in an application, such as your income and assets;
- Your name, address and telephone number (to the extent such information is not available from a public source);
- Your name, if it is included in a list of the company's customers;
- Details regarding your insurance coverage, including the premium you pay, the amount of coverage, etc.;
- Your premium payment history;
- Credit information, such as your credit history, that the company obtains from a consumer report.

11. Does this mean my insurer cannot sell my name, address and telephone number?

Your name, address and telephone number may or may not be protected depending on the context in which it is disclosed.

- If they are included in a list with other customers of the insurer, then they are protected information because it indicates that you are a customer of that insurer.
- If they are simply a random list of individuals whose information the insurer collected from public sources, then they are not protected, even if the list includes some of the insurer's customers.
- They would likely be considered protected information if they are included with other information such as your income, the amount of your insurance coverage, and your premium payments.

12. What does the term "non-public personal health information" mean?

Generally, **"non-public personal health information"** is any information that identifies you in some way, and includes information about your health, including your past and present physical and mental health, details about your health care, and payment for health care.

13. What are some examples of my "non-public personal health information"?

"Non-public personal health information" would include any document that gives enough information for the reader to identify you and includes information such as:

- Your medical records, which would have information regarding your general health (if you have a heart condition, asthma, cancer, AIDS, etc.);
- Information regarding your mental health; and
- Payment records, which could tell a great deal about your health by indicating, for example, the types of doctors you see, the types of medications you take, and the types of treatments you receive.

What are my Rights Under the New Law and Regulation?

14. What are the rules governing my financial information?

In general, insurers must:

- give you a copy of their privacy policy; and
- give you the opportunity to prohibit the sharing of non-public personal information with third parties.

Sharing information with affiliated companies is not prohibited, and the regulation contains extensive exceptions permitting the sharing of information for business purposes (like claims management), legal purposes (to comply with regulations and fight fraud, for example), and for certain marketing purposes.

The timing of your receipt of the privacy and opt out notices will differ depending on your relationship with your insurance companies and agents.

- If you are a "consumer" – for example, if you are in the process of applying for insurance – you will only receive the notices if the insurer wishes to disclose your personal financial information to a third party.
- At the time you become a "customer" – when an insurance policy is delivered to you, for example – the insurer must provide you with its privacy and opt out notices. Customers are entitled to receive privacy notices annually.

The insurer must give consumers and customers 30 days to respond to the opt out notice before sharing information with third parties.

15. What are the rules governing my health information?

Insurers must get your permission prior to disclosing your non-public personal health information to any other party. As with the financial information rules, there are exceptions that permit disclosure for business reasons (such as claims management and underwriting), and for legal reasons (like complying with regulations and fighting fraud).

16. Why do the rules governing health information differ from the financial information rules?

The health rules differ from the financial rules because state insurance regulators believe your health information is more sensitive than financial information and needs greater protections. That's why there is an affirmative consent requirement ("opt in") for health information as opposed to the "opt out" requirement for financial information. And consent is required before an insurer discloses health information to any other party – including affiliates and non-affiliated third parties. The "opt out" for financial information only applies to disclosures to non-affiliated third parties.

17. Even if I opt out, doesn't the company still need to share my information for certain purposes?

Yes, insurers will need to share some of your personal information and are permitted to do so whether or not you exercise your opt out and opt in rights. For example, your insurer can share your protected information to set underwriting rates, settle a claim made against your policy, investigate fraud, or comply with a legal order.

Privacy Notices and Opt Out Notices

18. When does my insurance company have to tell me about their privacy policy? Should I be worried if I don't receive something soon?

Your insurance company is required to inform you of its privacy policy, and give you an opportunity to opt out of the disclosure of your personal financial information to third parties, by July 1, 2001 (or the compliance date set by your state). After that date, your insurance company is required to send you a copy of its privacy policy every year.

In addition, if you become a consumer of a different insurance company after the compliance date – by submitting an application to that company, for example – that company must provide you with its privacy notice and an opportunity to opt out prior to disclosing any protected financial information to third parties.

Finally, although no privacy notices are required regarding health information, starting on the compliance date, insurers must get your permission before disclosing personal health information.

19. Do these new rules mean that I have to be given notice about an insurance company's privacy policy before they can sell me an insurance product?

Generally, insurers will have to provide you with their privacy and opt out notices prior to sharing your personal financial information. However, the exact timing of the delivery of the privacy and opt out notices may differ depending upon your relationship with the company. For example, when you are in the application process, you are entitled to receive the privacy and opt out notices only if the company wishes to share your information. In contrast, once you purchase the policy and it is delivered to you, the company must give you the notices.

Again, no privacy notices are required regarding health information, but starting on the compliance date insurers must get your permission before disclosing personal health information.

20. I'm in the process of applying for insurance. If my prospective insurance company is not required to give me a copy of its privacy policy because they don't intend to disclose the information, do I still have a right to request a copy of the policy? Is the company required to provide me a copy upon request?

You may request a copy of your insurer's privacy policy at any time, but the insurer is not obligated to provide it to you. Insurers are only required to give you their privacy policies under the following circumstances:

- If you are a consumer, they must provide you a copy prior to disclosing your protected financial information;
- If you are a customer, they must provide you a copy at the time that you become a customer, and annually thereafter.

21. I have my life insurance policy with one company, and my auto and homeowners' policies with another company. Will I receive a separate privacy notice for each policy? Will all privacy notices look the same? What should I be looking for when I receive the notice?

You will receive separate notices from each of the different insurance companies with which you do business, unless the companies are affiliated with each other in a large corporation. In that case, you might only receive one notice for all the policies held by those affiliated companies. The notice must clearly state to which companies and policies it applies.

Privacy notices will differ from company to company. However, there will be similar elements. First, they must be written so that they are noticeable and so you can read them clearly. For example, they cannot be in small type, hidden on the back side of a page in the middle of a large mailing. Second, they must contain similar information, including:

- the types of information the insurer collects about you;
- the types of information that the insurer discloses;
- the types of entities to which the insurer intends to give your information (including affiliates and third parties);
- the types of information and the entities to which the insurer intends to give your information for joint marketing purposes;
- how the insurer protects the confidentiality and security of your information; and
- an explanation of your right to opt out, including how you go about telling the insurer that you do not want your information shared with third parties.

22. I just received a privacy notice from my insurance company and it's very confusing. What do I do?

Your insurer should be able to explain to you exactly what their privacy policies mean and exactly what they intend to do with your personal information. In addition, your state insurance regulator can also help you to understand what privacy policies mean, and what protections you can expect under the law.

23. I just received a privacy notice from my insurer and initially thought it was junk mail. Isn't there a requirement to separate important information like privacy notices from other mailings?

Insurers are permitted to include privacy notices with other mailings. However, the privacy information must be written so that it is noticeable and so you can read it clearly. The notices cannot be in small type, hidden on the back side of a page in the middle of a large mailing, for example.

24. I just received a privacy notice from my insurance company that said they won't disclose any information about me except as permitted by law. This sounds good, but I've got no idea what's permitted by law. Does the law require them to disclose my information?

Insurers are permitted by law to disclose your information without your permission in a number of situations:

- They can share personal financial information with affiliated companies without restriction.
- They can share protected financial and health information for certain business reasons, including underwriting, settling claims, and investigating fraud.
- They could be required by law to disclose your personal financial or health information to an insurance regulator, court, or law enforcement official.
- They are permitted to disclose protected financial information without your permission pursuant to joint marketing or servicing agreements. This means that they can enter into agreements with third parties to share your financial information for (1) marketing certain products or services; or (2) hiring the third party to provide services for the insurer, like accounting and claims management.

25. What happens if I forget to send the opt out form to my insurer within the 30-day time period?

You may opt out at any time. However, if you fail to return an opt out form to your insurer within the initial 30-day time period, your insurer is permitted to share information with third parties. For example, if you send your insurer an opt out form 6 months after receiving the opt out notice, the insurer must stop disclosing your protected financial information to third parties as soon as the notice is received. But by that time, some of your protected information has probably been disclosed because the insurer has already had 5 months to share your information with third parties.

Beneficiaries and Claimants

26. My life insurance policy includes information about my spouse and children because they are my beneficiaries. Is their personal information protected?

Yes, if an insurer holds protected financial information about a named beneficiary of a life insurance policy and wishes to disclose that information to third parties, the insurer must provide the beneficiary with its privacy policy and the opportunity to opt out. If an insurer holds health information about a named beneficiary of a life insurance policy, the insurer must get the individual's consent prior to sharing that information with any other party.

27. I was in a car accident and my claim was paid by the other driver's insurer. That company now has information about me that I do not want disclosed. Can I do anything about that?

Financial Information: As a claimant under the other driver's policy, the other driver's insurance company may not disclose your financial information to third parties without giving you its privacy policy and an opportunity to prohibit such disclosure. The insurer may disclose financial information to its affiliates, however.

Health Information: The company may not disclose your health information to any party without your affirmative consent (except as permitted under one or more of the exceptions set out in the regulation).

Discrimination Prohibited; Reporting Illegal Disclosures

28. I am fearful of what might happen if I don't want my information shared. Can my insurance company raise my rates or drop my coverage if I opt out and stop the sharing of my financial information? Or if I don't allow the sharing of my health information by refusing to opt in?

Your insurer cannot discriminate against you for prohibiting the disclosure of your protected personal financial and health information by raising your rates or dropping your coverage. However, you might miss out on some of the benefits that other consumers receive as a result of allowing their personal information to be shared, such as special offers for various products and services.

29. What should I do if I think my information has been shared inappropriately? Who can help me find out what has happened?

If your insurance company or agent shares information in violation of their own insurance policy or in violation of the law, you should tell the company or agent and immediately report the violation to your state insurance commissioner. The commissioner has a variety of options under the law to stop illegal sharing of information and punish violations appropriately.

30. How do I contact my state insurance commissioner?

The name, address and phone number of every state insurance commissioner is available on the NAIC's website, which is located at *www.naic.org*. Click on "Insurance Regulators" and then on "Map of Insurance Regulators." Then click on your state, and you will be connected to your state insurance department's website.

Agent-Consumer Relationship

31. I never deal directly with an insurance company. I always go through my agent. Can I still do this?

Yes. These new privacy protections have no impact on your ability to work through your agent to obtain insurance coverage.

32. Do insurance agents have to follow the same rules as companies with respect to my information?

Yes, agents are required to comply with the law, just like insurance companies. So if your agent wishes to share your personal financial information with a third party (other than the insurance companies to which you are applying for coverage), the agent must give you a notice and the opportunity to opt out. If the agent wishes to share your health information with other parties (again, excluding insurance companies to which you are applying for coverage), the agent must obtain your consent.

Note that agents are not required to provide privacy and opt out notices for financial information, or obtain your consent for health information, if they are simply sharing information with insurance companies as part of the process of obtaining insurance coverage for you.

COMPANY ISSUES

Who must comply with the regulation?

1. Who is required to comply with the model regulations?

With some limited exceptions, all companies, agents and other persons and entities licensed under a state's insurance law are required to comply with the regulation, including health insurers and HMOs, which are considered "financial institutions" under GLBA.

2. My company provides title insurance. Are we required to comply with these new privacy regulations?

Yes. All entities licensed under the insurance law are required to comply with the regulation.

3. I'm an excess lines broker. Does the privacy regulation apply to me?

Yes, the regulation does apply to excess lines brokers. However, you are not required to comply with the financial information notice and opt out provisions if:

- you do not disclose any nonpublic personal information for any purpose including joint marketing and servicing, (except that you may disclose information pursuant to the specific business and legal exceptions); and
- you deliver a notice to your consumers and customers stating that fact.

4. Are insurance agents (producers) subject to the regulation?

Yes, see the "Questions for Agents" section for detailed information regarding the regulation's applicability to producers.

5. Are third party agents (TPAs) or managing general agents (MGAs) subject to the regulation?

All entities that are licensed under the applicable state insurance law are required to comply with the model regulation, including all licensed TPAs and MGAs.

6. Are workers' compensation plans covered by the regulation?

Yes, workers' compensation plans are subject to the regulation, although they are treated slightly differently from other insurers:

- **Financial Information:** A workers' compensation plan is only required to provide privacy and opt out notices to a person who receives benefits from the plan (a "beneficiary") if the plan wishes to disclose the beneficiary's nonpublic personal financial information to a third party outside the extensive exceptions provided in the regulation. In such a situation, the beneficiary is the plan's "consumer." Workers' compensation plans are also required to provide annual privacy notices to all plan participants.

- **Health Information:** Workers' compensation plans must comply with the same health privacy protections that apply to other insurers. Therefore, a workers' compensation plan must get the permission of a beneficiary before sharing that person's nonpublic personal health information (except when information is shared pursuant to one or more of the exceptions set out in the regulation).

Treatment of Consumers and Beneficiaries

7. How does the new regulation impact the disclosure of information about beneficiaries?

- For the treatment of **workers' compensation beneficiaries**, see question 6.

- A **beneficiary of a life insurance policy** is considered a consumer under the regulation if the insurer discloses nonpublic personal financial information about the beneficiary to a nonaffiliated third party outside the exceptions provided in the regulation. As a consumer, such a beneficiary is entitled to a privacy notice and the opportunity to opt out of the disclosure of nonpublic personal financial information.

- A **beneficiary of an employee benefit plan** is considered a consumer if the insurer discloses nonpublic personal financial information about the beneficiary to a nonaffiliated third party outside the exceptions provided in the regulation. As a consumer, such a beneficiary is entitled to a privacy notice and the opportunity to opt out of the disclosure of nonpublic personal financial information. Insurers are also required to provide annual notices to plan sponsors, regardless of whether they disclose beneficiary information to nonaffiliated third parties.

- **Health Information:** Insurers are required to get the consent of beneficiaries prior to disclosing nonpublic personal health information to any other party (except when information is shared pursuant to one or more of the exceptions set out in the regulation).

8. How does the new regulation impact the disclosure of information about claimants?

- **Financial Information:** A claimant under any insurance policy is considered a consumer under the regulation if the insurer discloses nonpublic personal financial information about the claimant to a nonaffiliated third party outside the exceptions provided in the regulation. As a consumer, such a claimant is entitled to a privacy notice and the opportunity to opt out of the disclosure of nonpublic personal financial information.

- **Health Information:** Insurers are required to get the consent of claimants prior to disclosing nonpublic personal health information to any other party (except when information is shared pursuant to one or more of the exceptions set out in the regulation).

9. What if my company has nonpublic personal information about a claimant and does not share it?

Your company has no obligations to a claimant if you do not share nonpublic personal financial information with third parties or nonpublic personal health information with any other party.

10. What if my company has nonpublic personal information about a beneficiary and does not share it?

Your company has no obligations to beneficiaries if you do not share their nonpublic personal financial information with third parties or nonpublic personal health information with any other party. However, companies are required to provide initial, annual and revised privacy notices to employee benefit plan sponsors, group or blanket insurance policyholders, group annuity contractholders and workers' compensation plan participants (employers).

11. My company provides on-going settlement options for beneficiaries and claimants. If a beneficiary or claimant takes advantage of such an option, is that person a consumer or a customer?

Beneficiaries and claimants that submit a claim under a policy choosing a settlement option involving an on-going relationship with an insurer are considered consumers, not customers. Thus, the company will be required to provide the individuals with privacy notices and an opportunity to opt out if the company wishes to disclose the individual's nonpublic personal information to third parties. Affirmative consent is required for the disclosure of health information. There are no on-going privacy policy notice requirements.

Effective Date and Compliance in Absence of Regulations

12. The effective date for Title V of the Gramm-Leach-Bliley Act, which contains the Act's privacy provisions, was November 13, 2000. I'm concerned, however, because several of the states in which my company does business do not have privacy regulations in effect. Could a state insurance regulator or attorney general bring an enforcement action against my company for not complying with GLBA, even though there are no regulations to instruct us as to how to comply?

In June 2000, every state insurance regulator endorsed an NAIC resolution that pledges to delay the compliance date for the GLBA privacy regulations until July 1, 2001 (that is the same compliance date that federal financial services agencies have set forth in their regulations). In addition, most states have issued emergency regulations or bulletins saying the same thing. Finally, even in the absence of an emergency regulation or bulletin, it is not clear that a state regulator or attorney general would have authority to enforce a federal law in the absence of some sort of state action, such as a statute or regulation.

13. What happens if a state in which my company does business hasn't issued a privacy regulation by July 1, 2001?

If your company does business in a state that has not issued a privacy regulation by July 1, 2001, you should consider complying with the privacy regulation of your company's state of domicile. The model regulation provides that a company that is in compliance with its domiciliary state's regulation could be deemed to be in compliance with GLBA's privacy provisions in states that have no regulation. Although it is not binding in a state that has not promulgated a final regulation, this provision is intended to give insurers some guidance for complying with GLBA in such states.

Interaction with U.S. Department of Health and Human Services Health Privacy Regulation

14. My company is required to comply with the health information privacy regulations issued by the U.S. Department of Health and Human Services (HHS) pursuant to the Health Insurance Portability and Accountability Act (HIPAA). We are concerned about dual regulation and complying with both the HHS regulation and the NAIC model regulation. What should we do?

Under the model regulation, you are required to meet the requirements of the health privacy provisions from the July 1, 2001 compliance date until you are in compliance with the HHS regulation. Once your company is in compliance with the HHS regulation, you are no longer required to comply with the NAIC model regulation. Thus, there will be no danger of having to comply with both the HHS regulation and the NAIC model regulation at the same time.

In addition, there is little danger of the two regulations conflicting. Not only are companies permitted to comply with the HHS regulations in lieu of the NAIC model regulation, but the health information requirements of the NAIC model regulation are very bare bones. The regulation simply requires consent prior to disclosing health information. Companies are free to establish their own mechanisms for complying, or they may implement the more detailed compliance requirements of the HHS regulation.

15. My company is not required to comply with the HHS regulation, but we prefer the HHS regulation to the NAIC model regulation. Do we have any options?

Yes, you can comply with either the HHS regulation or the NAIC model regulation. If you are in compliance with the HHS regulation – even if you are not required to comply with that regulation – you are not required to comply with the NAIC model regulation.

Treatment of Health Information

16. What are the requirements for the disclosure of health information to affiliates?

You must get the consent of the consumer or customer before disclosing health information to affiliates (or third parties). Note that there are extensive exceptions to that general rule so that information can be disclosed to affiliates and others for legitimate business purposes, such as claims handling, underwriting, and fraud investigation, and for legal and regulatory purposes.

17. Although there are many specific exceptions to the rule requiring affirmative consent prior to the disclosure of health information, what happens if a situation arises in which there is a real need to disclose information but it does not fall into one of the exceptions?

In the absence of the individual's consent and a specific exception, there are two "catch-all" exceptions to the opt in rule that may be applicable:

- Any exception in the HHS regulations that is not specifically stated in the NAIC model regulation is incorporated by reference in the model regulation. So, if an HHS regulation exception applies to your situation, no affirmative consent by the individual is required. This is true even if you are not otherwise in compliance with the HHS regulation.

- If none of the specific exceptions in the NAIC model regulation or the HHS regulation apply, you may request that the commissioner add an exception. The NAIC model permits such additions if they are "necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers."

18. I know my company must send privacy notices to customers and certain consumers regarding financial information, but are we required to send notices to customers and consumers if we only have health information about them?

No. The notice provisions of the model regulation do not apply to health information. The only time you are required to disclose the types of health information you possess and what you are going to do with that health information is when you contact consumers and customers to ask them to consent to the disclosure of such information.

Privacy Policy Notices

19. To whom do we have to give annual privacy policy notices?

Insurers are required to provide their customers with annual privacy notices. "Customers" are individuals with whom you have on-going relationships. Policyholders are customers, for example. In contrast, applicants are consumers and are only entitled to privacy notices if you wish to share their protected financial information with third parties. Similarly, beneficiaries and claimants are only entitled to receive privacy notices if you wish to disclose their protected information with third parties.

20. What happens if my company does not get privacy notices to all of our customers by July 1, 2001?

If you have not sent privacy notices to all your customers by July 1, 2001, you will be in violation of the model regulation. A violation of the regulation will be considered a violation of the state unfair trade practices act or similar law, depending upon the state in question. State insurance departments have many avenues available to enforce such laws. The type of enforcement action will depend upon the severity of the violation.

21. What happens if I forget to give a privacy notice to a consumer?

You are not required to give a privacy notice to a consumer unless you wish to disclose nonpublic personal financial information regarding that consumer to a nonaffiliated third party. So, if you do not give the consumer a notice and do not disclose his or her information to a third party, there is no problem. If, however, you do not give the consumer a notice and you do disclose his or her information to a third party, you would be in violation of the regulation and subject to applicable enforcement actions.

22. Can we send privacy notices, opt out notices and opt in notices together in the same mailing? Can they be sent with other customer mailings?

Privacy, opt out and opt in notices can be sent together or separately, and they can be sent with other customer mailings. In addition, affiliated companies may send notices together, or they can send combined notices. No matter how they are sent, however, all notices must identify the companies and policies to which they apply. They must be accurate, and they must be clear and conspicuous so that the customer can read and understand them.

Disclosure to and from Other Parties

23. My company hires insurance agents to service transactions and perform services on our behalf. Can we disclose nonpublic personal information to such agents?

Yes. A company can share nonpublic personal information with service providers for a variety of purposes regardless of whether a consumer permits disclosure of his or her information.

Section 14 of the model regulation specifically permits companies to share nonpublic personal financial information with third parties to enable them to perform services for the company or functions on the company's behalf. The only requirements are (i) the company must provide an initial notice to the individual, and (ii) the company must enter into a written agreement with the third party prohibiting the third party from using the information other than to carry out the purposes for which the information was disclosed and pursuant to the exceptions in the rule.

Section 15 of the model regulation permits companies to share nonpublic personal financial information with third parties, including agents, for numerous servicing purposes including: servicing or processing an insurance product that a consumer requests or authorizes; carrying out the service business of which the consumer's transaction is a part; and administering or servicing benefits or claims. Such disclosures are subject to the model regulation's reuse and redisclosure provisions, which generally prohibit third parties that receive information under an exception from using such information other than to carry out the purposes for which the information was disclosed and pursuant to the exceptions in the rule.

Section 17 of the model regulation permits companies to share nonpublic personal health information with affiliates and third parties, including agents, for numerous business activities such as claims administration, fraud reporting, and policy placement and issuance.

24. My company consists of many affiliated insurers. Some of our employees are actually employed by several of the affiliated companies at the same time. Suppose an employee works for Companies A, B, C and D, and holds protected health information about a customer of company A. The customer has not consented to the disclosure of protected health information. Is that employee in violation of the model regulation?

No, the employee is not in violation of the regulation simply by virtue of his or her employment status and knowledge of information. However, the employee (and thus the insurer) would be in violation if the employee uses the protected health information of Company A's customer on behalf of Company B, C or D outside one of the exceptions to the general rule. In that way, the employee would be "disclosing" the information to the other company.

25. Does my company have any obligations once we have disclosed information to a third party?

No, but the third party's use and disclosure of that information is limited.

26. What are our obligations if we receive nonpublic personal information from another entity?

If your company receives nonpublic personal financial information from a nonaffiliated financial institution, your use and disclosure of that information is limited as follows:

- you may disclose the information to the original financial institution's affiliates;
- you may disclose the information to your affiliates, but they, in turn, may only disclosure the information to the extent you may disclose the information;
- if you received the information pursuant to one of the exceptions in the model regulation, you may use and disclose the information pursuant to an exception in the ordinary course of business to carry out the activity covered by the exception under which you received the information; and
- if you received the information outside an exception, you may disclose the information to any other person if the original financial institution could lawfully disclose the information to that person.

27. My company receives information from banks and securities firms that are subject to separate privacy regulations. What rules do we follow with respect to this information?

When you receive information from another financial institution, such as a bank or securities firm, that information may be subject to the regulations that govern the institution. The Federal Reserve Board, the Office of the Comptroller of the Currency, and the Federal Trade Commission are just three of the several federal government agencies that have promulgated privacy regulations for financial institutions under GLBA.

All of the federal regulations contain provisions restricting the reuse and redisclosure of protected information by parties that receive information from financial institutions. These provisions are identical in all material respects to the reuse and redisclosure provisions in the NAIC model regulation. Generally, they permit you to disclose protected information received from another financial institution only to the extent the original financial institution could disclose the information. (See question 26 for further details.)

Note that receipt of such information could also give rise to obligations under the insurance privacy regulation if the information involves one of your consumers or customers.

Discrimination

28. If my company is unable to process a claim because an individual has "opted out" of disclosure, could we be in violation of the regulation's discrimination provision?

These two issues are not related. The fact that an individual has "opted out" of disclosure will have no impact on your company's ability to handle claims or do any other business activity related to servicing or processing a particular product or service. The extensive business exceptions to the rule ensure that companies can continue these standard business operations without interruption. Because your company will be able to process claims, the discrimination issue will never arise.

29. Can my company charge lower rates to policyholders that permit their information to be shared?

No, premium rates cannot be based on an individual's choice to prohibit or allow the sharing of his or her information. However, this does not prevent a company from offering discounts for other reasons.

30. There is no non-discrimination clause in the federal privacy regulations. Why does the NAIC model include such a provision?

By its nature, insurance treats people differently depending on their circumstances. For example, life insurance premium rates may differ depending on age, health, and gender. Homeowner's insurance rates may differ depending on the value and location of the home. An individual's choice to protect his or her personal information, however, is not a legitimate factor in determining an appropriate underwriting rate. People should not feel pressured to "sell" their private information in order to get cheaper insurance.

Note that the non-discrimination provision of the model regulation prohibits "unfair discrimination." Although insurers cannot discriminate against consumers and customers for prohibiting the disclosure of their personal information by raising rates or dropping coverage, insurers don't have to offer them the special offers that are available to consumers and customers who permit their personal information to be disclosed.

AGENT ISSUES

1. **Does the NAIC model "Privacy of Consumer Financial and Health Information Regulation" apply to agents?**

Yes, the model regulation does apply to agents. However, an agent does not have to comply with the notice and opt out requirements of the regulation if:

- the agent is an employee, agent or other representative of another licensee (a "principal") that complies with, and provides the notices required by, the regulation; and
- the agent does not disclose protected information to any person other than the principal or its affiliates.

So, if an agent wishes to disclose a consumer's protected information to an entity other than the insurance company that the agent is representing, the agent must give the consumer a copy of the agent's privacy notice and an opportunity to prohibit the disclosure of that information to non-affiliated third parties ("opt out").

2. **I'm a paid representative of one insurance company and I only represent that company and its line of insurance and financial services products. What are my responsibilities under this new privacy rule?**

You are subject to the regulation, but you are not required to comply with the notice and opt out requirements of the regulation if:

- the company for which you act as an agent complies with the regulation; and
- you do not disclose protected information to any person other than that company or its affiliates.

3. **I'm an independent agent and therefore represent a variety of insurance companies. What are my responsibilities under the privacy rule?**

Just like other agents, you are subject to the regulation, but you are not required to comply with the notice and opt out requirements of the regulation if:

- the company (or companies) for which you are acting as an agent with respect to a particular consumer complies with the regulation; and

- you do not disclose protected information to any person other than that company (or companies) or the affiliates of that company (or companies).

4. I am a licensed insurance agent and I sell variable annuities. Am I required to comply with the privacy rule?

Yes, you are subject to the model regulation. However, just like other agents, you are not required to comply with the notice and opt out requirements of the regulation if:

- the company (or companies) for which you are acting as an agent with respect to a particular consumer complies with the regulation; and
- you do not disclose protected information to any person other than that company (or companies) or the affiliates of that company (or companies).

5. I'm an independent agent and need to share consumer information with many insurers in order to get the best prices for my clients. Is this permissible under the privacy regulation?

Yes, an agent may share protected information with multiple companies in an effort to compare prices. In such situations, the individual will be a consumer of each of the companies and will be entitled to privacy and opt out notices from any of the companies that wishes to share the individual's protected financial information with non-affiliated third parties. The individual's consent will be required prior to disclosure of protected health information.

Note that these individuals may become your consumers – or customers – if you disclose their protected information. (See question 1.)

6. Do I have to go back to every one of my existing clients and tell them about this new rule?

Not necessarily. You are required to provide privacy and opt out notices and opt out opportunities to a client if the client is your "customer." A client is considered your customer if he or she obtains financial, investment or economic advisory services relating to an insurance product or service from you for a fee, or if the individual obtains insurance through you.

If you are acting as agent for another licensee (a "principal"), however, you are not required to provide privacy notices to your customer if:

- the principal complies with the regulation with respect to that customer; and
- you do not disclose protected information about that customer to any person other than the principal or its affiliates.

If you are required to send privacy and opt out notices to existing clients, they must be sent by July 1, 2001, which is the compliance date set forth in the model regulation. (Note that states may have later compliance dates, depending upon when they promulgate their regulation.)

It is important to note that starting on the compliance date, all new clients will be either consumers or customers, and will be entitled to the privacy and opt out notices required by the regulation. (See questions 1-4 for an explanation of whose responsibility it is to provide those notices.)

7. Every company is different. Of the companies I represent, how am I supposed to know which ones sent out notices?

Like all aspects of the agent-principal relationship, effective compliance with privacy regulations will require on-going communication and coordination between the parties.

8. What if one of my clients didn't receive a notice from a company? Who is responsible?

Specific compliance issues will be decided on a case-by-case basis, of course. However, if an agent is acting in good faith and legitimately relies on a company to comply with the regulation, the agent would have a good argument that he or she should not be held responsible. (See questions 1-4.)

9. Our agency receives phone-in requests for information on the insurance products offered by the companies we represent. Do we have to tell these callers the privacy policy of each of the companies when they call in?

Not necessarily. If these individuals are simply requesting information and not purchasing a product, they are likely to be considered consumers – either your consumers or consumers of the companies for which you are acting as agent. If you collect protected personal information about these individuals and you are going to share that information with non-affiliated third parties, you will be required to provide them privacy and opt out notices prior to disclosure of any protected personal information. On the other hand, if you are not going to disclose any non-public personal information to non-affiliated third parties, you have no obligations to provide privacy and opt out notices to the individual. Finally, if you are going to disclose information only pursuant to a joint marketing or servicing agreement, a privacy notice is all that is required; the consumer is not entitled to opt out.

If an individual actually purchases a product from you over the telephone, that individual is considered a customer. Normally, customers are entitled to privacy and opt out notices at the time the customer relationship is established. With a telephone transaction, however, delivery of notices can be delayed with the customer's consent.

The same obligations would apply to the companies for which you are acting as agent.

10. I'm an independent agent and I perform servicing and processing functions for several insurers. Does the model regulation permit the exchange of information necessary for me to continue to perform these functions?

Yes. An insurer can share nonpublic personal information with agents acting as service providers for a variety of purposes regardless of whether a consumer permits disclosure of his or her information.

Section 14 of the model regulation specifically permits companies to share nonpublic personal financial information with third parties to enable them to perform services for the company or functions on the company's behalf. The only requirements are (i) the company must provide an initial notice to the individual, and (ii) the company must enter into a written agreement with the third party prohibiting the third party from using the information other than to carry out the purposes for which the information was disclosed and pursuant to the exceptions in the rule.

Section 15 of the model regulation permits companies to share nonpublic personal financial information with third parties, including agents, for numerous servicing purposes including: servicing or processing an insurance product that a consumer requests or authorizes; carrying out the service business of which the consumer's transaction is a part; and administering or servicing benefits or claims. Such disclosures are subject to the model regulation's reuse and redisclosure provisions, which generally prohibit third parties that receive information under an exception from using such information other than to carry out the purposes for which the information was disclosed and pursuant to the exceptions in the rule.

Section 17 of the model regulation permits companies to share nonpublic personal health information with affiliates and third parties, including agents, for numerous business activities such as claims administration, fraud reporting, and policy placement and issuance.

Senate Bill 2127 amendment proposed by Blue Cross Blue Shield of North Dakota.

On line 12 add the following language after 'section.' "An insurer that is required to be in compliance with Health Insurance Portability and Accountability Act (HIPAA) is not subject to the provisions of SB2127 until 8/1/03.

This amendment is requested by the American Insurance Association and submitted to the Senate Industry, Business and Labor Committee by Leah K. Coghlan of Pearce & Durick.

PROPOSED AMENDMENT TO
SENATE BILL NO. ~~2358~~ 2127

On line 12, following "section.", insert the following language:

Such rules and regulations shall be consistent with and not more restrictive than the model regulation adopted by the National Association of Insurance Commissioners entitled "Privacy of Consumer Financial and Health Information Regulation." Nothing in this section shall be construed to create a private right of action.