

FREQUENTLY ASKED QUESTIONS

NAIC PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION MODEL REGULATION

Table of Contents

Overview.....	3
Glossary of Terms.....	4
Consumers Issues.....	5
?? New Law Governing Insurers Protects Your Privacy.....	6
?? What Information is Protected under the New Law and Regulation?.....	8
?? What are my Rights Under the New Law and Regulation?.....	10
?? Privacy Notices and Opt Out Notices.....	11
?? Beneficiaries and Claimants.....	14
?? Discrimination Prohibited; Reporting Illegal Disclosures.....	15
?? Agent-Consumer Relationship.....	15
Company Issues.....	17
?? Who Must Comply with the Regulation.....	18
?? Treatment of Consumers and Beneficiaries.....	19
?? Effective Date and Compliance in Absence of Regulations.....	20
?? Interaction with U.S. Department of Health and Human Services Health Privacy Regulation.....	21
?? Treatment of Health Information.....	22
?? Privacy Policy Notices.....	23
?? Disclosure to and from Other Parties.....	24
?? Discrimination.....	26
Agent Issues.....	27

Overview

The NAIC adopted the Privacy of Consumer Financial and Health Information Model Regulation on September 26, 2000. The model regulation was drafted in response to requirements set forth in Title V of the Gramm-Leach-Bliley Act (P.L. 106-102) (GLBA), which was signed into law by President Clinton on November 12, 1999. GLBA calls on the state insurance regulators to issue regulations protecting the privacy of insurance consumers' personal information.

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 non-affiliated third parties; and
- (3) obtain affirmative consent from consumers before sharing protected health information with any other parties, affiliates and non-affiliates 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.

The following frequently asked questions and answers have been prepared by NAIC staff in order to give some guidance to those interested in learning about how the model regulation works. The answers to these questions are only applicable to the model regulation. They do not represent the views of any particular state insurance regulator. The answers contained herein do not have the force of law and are not meant to supersede any guidance that might be provided by the individual states when they issue their regulations.

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 disclose 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.

Filename: 1-4-01 FAQ.doc
Directory: C:\DOCUME~1\rob\LOCALS~1\Temp
Template: C:\Documents and Settings\rob\Application
Data\Microsoft\Templates\Normal.dot
Title: Overview: Consumer Privacy Protections Handbook
Subject:
Author: jfielding
Keywords:
Comments:
Creation Date: 1/4/2001 10:17 AM
Change Number: 36
Last Saved On: 1/12/2001 5:28 PM
Last Saved By: jfielding
Total Editing Time: 439 Minutes
Last Printed On: 2/16/2001 2:14 PM
As of Last Complete Printing
Number of Pages: 31
Number of Words: 8,684 (approx.)
Number of Characters: 49,503 (approx.)