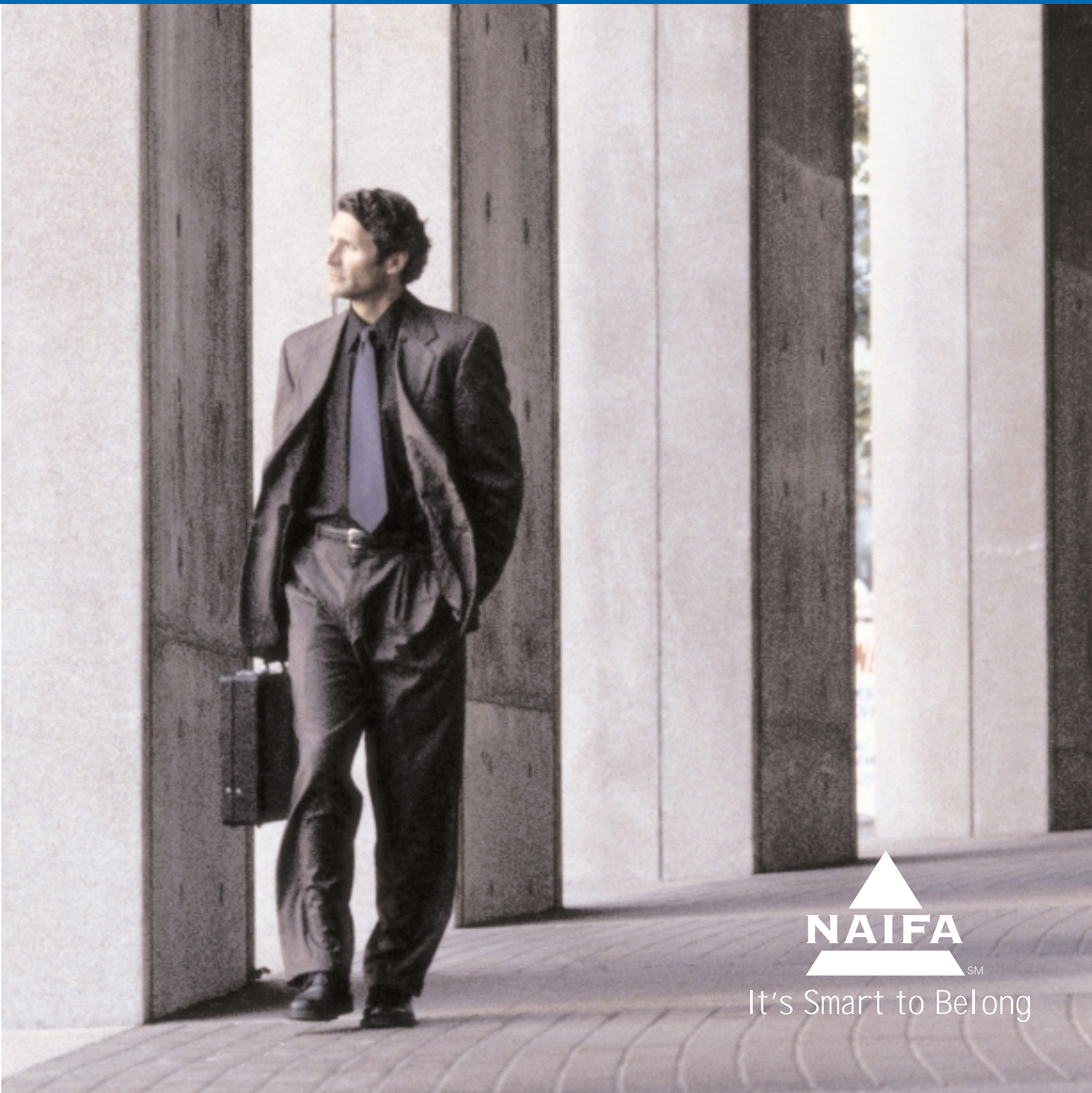


Insurance Producer Privacy Guide



It's Smart to Belong

Table of Contents

Introduction & Purpose of this Guide	1
Appendix 1	23
Appendix 2	29
Appendix 3	43
Appendix 4	47
Appendix 5	57
Appendix 6	73
Appendix 7	83
Appendix 8	91
Appendix 9	99
Appendix 10	115
Appendix 11	123
Appendix 12	133
Appendix 13	149

Introduction and Purpose of this Guide

This Guide is designed to assist agencies in complying with:

- the Gramm-Leach-Bliley Act (“GLBA”) information handling privacy obligations;
- the Fair Credit Reporting Act (“FCRA”) privacy requirements;
- the Health Insurance Portability and Accountability Act (“HIPAA”) requirements; and
- the European Union (“EU”) Privacy Directive protection requirements.

As a general matter, the GLBA imposes three overarching privacy obligations:

- (1) **Privacy Notice Disclosure Requirement.** Every insurance agency must provide all of its “customers” with an annual notice that describes the manner in which their nonpublic personal information is collected, maintained and disseminated.
- (2) **Opt-Out Notification Requirement.** Before sharing “nonpublic personal information” about a “consumer” with a non-affiliated third-party for a “non-exempted purpose,” the “consumer” must be notified of the right to prohibit the sharing of that “nonpublic personal information” for a “non-exempted purpose” (an “opt-out” right).
- (3) **Data Security and Integrity Requirement.** All agencies that collect or maintain consumer’s nonpublic personal information must institute mechanisms for protecting the security and integrity of that information. Security mechanisms are designed to protect the information from inadvertent disclosures. Integrity mechanisms, in contrast, are intended to protect nonpublic personal information that is maintained in an electronic medium from becoming corrupted. The rules do not, however, dictate that any specific mechanisms be instituted.

The specific parameters of these requirements are discussed in Part I of this Guide.

The FCRA, in contrast, requires that individuals be permitted to “opt-out” before personal, “non-transactional” information may be shared with an “affiliate” if that information is intended to be used for an insurance, credit or employment-related purpose. The specific parameters of this “affiliate” “opt-out” requirement are discussed in Part II and in Appendix 8 of this Guide.

HIPAA uses an “opt-in” standard to regulate most uses and disclosures of individual-

ly identifiable health information, whether oral, electronic or recorded in any form. The HIPAA rules apply to a variety of persons and entities that are exposed to such information, including all health insurance agents. The HIPAA regulations do not apply, however, to agents to the extent that they sell certain “excepted benefits,” including life, disability, automobile, property and casualty, and workers compensation insurance. The specific parameters of the HIPAA opt-in requirement and the situations in which it applies are discussed in Appendix 12 of this Guide.

The EU Privacy Directive prohibits the transfer of “personal data” to non-EU nations that do not meet the EU “adequacy” standard for privacy protection. There are several mechanisms available for complying with these requirements. The specific parameters of the Directive and of the “Safe Harbor” compliance requirements are outlined in Appendix 11 of this Guide.

Before reviewing the specific parameters of each of these sets of privacy requirements, a few caveats are appropriate. **First, only the information of individuals that is used for personal, family or household purposes is regulated under each of these privacy regimes; information regarding businesses is not protected in any way.**¹

Second, the States are required to implement, interpret and enforce the GLBA privacy requirements for insurance producers and carrier. The federal banking and securities agencies and the Federal Trade Commission (“FTC”) have that authority for banks and other financial institutions within their respective jurisdictions. Although each of the federal agencies has issued its final regulations implementing the GLBA provisions, only four States have issued final GLBA requirements – Iowa, New Hampshire, New York and Washington. It is expected that there will be GLBA privacy legislative and regulatory activity in every other State shortly and that the final GLBA requirements in each of those States will be closely based on one of two models – one issued by the National Association of Insurance Commissioners (“NAIC”) and a second issued by the National Conference of Insurance Legislators (“NCOIL”).

Although there will be a strong industry effort to ensure that the models are enacted in each State without modification, it is impossible to predict what the final requirements in each State will be because of the varying dynamics of each State’s political processes and because the GLBA authorizes States to impose more protective privacy requirements than the GLBA requirements. This uncertainty is compounded by the fact that 17 States previously enacted insurance-specific privacy statutes or regulations that will need to be modified or replaced in light of the GLBA privacy mandate. For that reason, **THE GLBA**

¹ This means that information gathered in connection with commercial coverages, including directors and officers insurance or keyman insurance, is **not protected**.

COMPLIANCE INFORMATION INCLUDED IN THIS GUIDE SHOULD BE VIEWED AS AN INTRODUCTION TO AND AN OUTLINE OF AN AGENCY'S POTENTIAL OBLIGATIONS. EACH AGENCY WILL HAVE TO ENSURE THAT IT IS IN COMPLIANCE WITH THE REQUIREMENTS THAT ARE ULTIMATELY ENACTED IN ANY STATE IN WHICH IT ENGAGES IN INSURANCE PRODUCER ACTIVITIES.

Third, it appears that **the date by which agencies will need to be in compliance with the GLBA privacy obligations is July 1, 2001.** Under the GLBA, the intended compliance date was November 12, 2000 but the federal agencies and almost every State extended that date to July 1, 2001. Unfortunately, many of the state rules may not be finalized until shortly before they become effective, which will not leave much time to become compliant. For that reason, agencies should begin determining how to comply as soon as possible, and then finalize their compliance practices after the final privacy regulations that govern their activities are available.

The Guide itself is composed of this memorandum and of twelve Appendices. This memorandum is divided into two parts:

- **Part I** – explains the key elements of the GLBA notice and opt-out privacy obligations and provides guidance for complying with these obligations.
- **Part II** – outlines the related FCRA opt-out notice requirements and provides guidance for compliance.

The Appendices include model provisions that agencies can use to satisfy their compliance obligations and memoranda with more in-depth analyses of important issues:

- **Appendix 1** – contains a master model GLBA privacy policy disclosure form.
- **Appendix 2** – contains sample clauses that can be inserted into the Appendix 1 form in accordance with an agency's specific information collection and disclosure practices.
- **Appendix 3** – contains a sample opt-out form.
- **Appendix 4** – discusses the GLBA "service provider/joint marketing" exceptions to the GLBA "opt-out" requirement and includes a sample contract provision that can be used to qualify for this exception.
- **Appendix 5** – provides an in-depth, provision-by-provision analysis of the NAIC GLBA privacy model.
- **Appendix 6** – outlines the additional obligations imposed in States that have enacted the 1982 NAIC Insurance Information and Privacy Protection Act.

- **Appendix 7** – contains a sample privacy notice that satisfies both the GLBA and the 1982 NAIC Model Insurance Information and Privacy Protection Act, and should be used in lieu of the form in Appendix 1 by agencies doing business in 1982 Act States.
- **Appendix 8** – outlines FCRA regulations that have been proposed by the FTC (and that will apply to insurance producers if adopted) and expands upon the FCRA discussion.
- **Appendix 9** – discusses the requirements of the EU Safe Harbor.
- **Appendix 10** – includes suggested guidelines for complying with the GLBA data security and integrity requirements.
- **Appendix 11** – describes the requirements for complying with the Federal Electronic Signatures Act, which are important for agencies that conduct business and provide disclosure notices electronically (via email or a web site).
- **Appendix 12** – provides a summary of the new health information privacy regulations under the HIPAA with respect to sales of health insurance benefits to individuals.²
- **Appendix 13** – includes a suggested list of audit questions that can be used to help bring agencies into compliance with the GLBA, FCRA and EU privacy requirements.

INSTRUCTIONS FOR USING THIS GUIDE

The privacy rules outlined in this Guide can be both cumbersome and complex. In addition, the Guide has been written to provide guidance to both small, stand-alone agencies that do not share any information at all other than to place initial coverages as well as to large, multi-national agencies that engage in a full panoply of financial services (and information sharing) activities. We have attempted to make the Guide more accessible regardless of your agency's size and breadth of activities by presenting the information in a modular format that relies heavily on the Appendices listed above.

The Appendices can be divided into two categories: (1) Appendices 4, 5, 6, 8, 9, 11 and 12 are memoranda that explain an agency's obligations under various privacy statutes or regimes in more detail than is provided in this cover memorandum; and (2) Appendices 1, 2,

² Appendix 12 does not address group health sales. The group health plan rules are extremely detailed and complex and require a separate analysis. We will provide a separate analysis of the group health plan rules in the near future.

3, 7, 10 and 13 are sample clauses, forms or guidelines that will help agencies implement these obligations. Not all agencies will need to refer to all 13 Appendices, because they each address different facets of the privacy laws – and not all of these laws apply to everyone.

Here is a list of an agency's basic compliance obligations and the parts of this Guide that should be referenced by agency activity:

- (1) *Agencies that place non-health insurance primarily for one carrier and do not share non-public personal information with any third party other than carrier and its affiliates (i.e. life agents) – only obligation is to give the core privacy notice; may qualify for use of the agent exemption. (See Part I of this Memorandum and Appendices 1 and 2).*
- (2) *Agencies that place non-health insurance with multiple carriers and that seek competitive bids to replace non-health coverages (i.e. independent property and casualty agents) – must give the core privacy notice and enter into joint marketing agreements with each carrier for which the agency is appointed. (See this Memorandum and Appendices 1, 2 and 4).*
- (3) *Agencies that fall under Scenario (1) or (2) but also engage in a broader range of information sharing with non-affiliated third-parties that are not insurance companies – in addition to the requirements listed above, must also provide an “opt-out” notice and may be required to comply with the Fair Credit Reporting Act obligations. (See Parts I and II of this Memorandum and Appendices 3 and 8).*
- (4) *Agencies that fall under any of the Scenarios (1) – (3) that are servicing customers in “1982 NAIC Model Act” States³ – must comply with the 1982 Act requirements. (See Appendices 6 and 7).*
- (5) *Agencies that fall under any of the Scenarios (1) – (4) that are selling or servicing health insurance policies or programs – must also comply with the new HIPAA medical information protection provisions. (See Appendix 12).*
- (6) *Agencies that fall under any of the Scenarios (1) – (5) that are receiving non-public personally identifiable information from the European Union – must also comply with the new EU data protection requirements. (See Appendix 9).*
- (7) *Agencies that fall under any of the Scenarios (1) – (5) that conduct business electronically and provide disclosure notices electronically – must also comply with the requirements of the Federal Electronic Signature Act. (See Appendix 11).*

³ The 16 States are: Arizona, California, Connecticut, Georgia, Illinois, Kansas, Maine, Massachusetts, Minnesota, Montana, Nevada, New Jersey, North Carolina, Ohio, Oregon, and Virginia.

Finally, all agencies should refer to Appendices 10 and 13 for guidelines that are useful to consider in the course of discharging the above-mentioned compliance obligations. Appendix 10 contains suggested guidelines for complying with the GLBA data integrity and security requirements. Similarly, Appendix 13 contains a suggested list of audit questions that can be used to help bring agencies into compliance with the GLBA, FCRA and EU privacy requirements.

PART I – THE GLBA PRIVACY REQUIREMENTS

A. INTRODUCTION

The GLBA imposes three overarching privacy obligations: (1) providing a notice of the agency's nonpublic personal information handling practices; (2) providing an "opt-out" right before information can be shared with non-affiliated third parties for a "non-exempted" purpose, and (3) instituting data security and integrity mechanisms to protect nonpublic personal information. There are, however, two preliminary issues to address – who must comply and what type of information is protected under the "opt-out" right.

1. Who Must Comply?

All insurance producers are required to comply with the GLBA privacy requirements unless they qualify for the insurance agent exception described below that is included in both the NAIC and NCOIL model privacy acts. This is because the proposed NAIC and NCOIL model GLBA provisions apply to all insurance "licensees." A "licensee" is defined as any person or entity that is licensed by a State's department of insurance.

Under the NAIC and NCOIL "agent" exception, however, a "licensee" is not subject to the GLBA privacy notice requirements governing financial information if three conditions are met:

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

An insurance agency can qualify for this exception – and not be required to issue the GLBA initial or annual privacy notice – for any transaction on which it is acting as an agent for an insurance company, as long as the agency does not disclose any nonpublic personal information about that customer to any third party except the insurance carrier or its affili-

ates. In effect, the agent exception excuses any agency that limits its information sharing to insurance companies from compliance with the GLBA privacy notification burdens.

The agent exception to the GLBA notice requirements benefits agents in at least two situations. First, it benefits agencies with exclusive agency relationships with an insurance company – such as most life insurance agents. In many cases, however, such agencies may be better off agreeing to be covered by that company's GLBA privacy policy.

Second, the agent exception benefits agents involved in more traditional types of agency activities who do not share protected information with third parties post-sale. Specifically, if an agent submits an individual's applications to a number of different insurance companies to solicit bids, that individual is not a customer until an application is accepted and the individual becomes a policyholder of the insurance company. Post-sale, as long as the agent does not share that individual's information with anyone other than the insurance company or its affiliates, it is not required to provide its own notice or opt-out. If, however, the agency intends to solicit competitive bids or renewals, it will be required to issue privacy notices, and it should review the "joint marketing" requirements and procedures addressed in Appendix 4.

Any agent seeking to take advantage of this exception in order to eliminate or reduce its GLBA compliance burdens should ensure that its appointment contracts specifically require the carrier to be in compliance with its GLBA obligations. In addition, agents should note that, even if they qualify for the agent exception, the data security and integrity requirements still apply. Finally, it is important to note that some of an agency's nonpublic personal information handling activities may qualify for this exemption, while other of its nonpublic personal information handling activities may not. For example, an agency that also engages in insurance broker services (such as providing advice to customers or negotiating on their behalf) is not exempt from providing the initial and annual privacy notices to its broker customers because a broker does not act as an agent of another licensee when it is performing brokerage services.

2. What Type of Information is Protected?

The cornerstone of the GLBA privacy obligations is the protection of "nonpublic personal information." Understanding what type of information counts as nonpublic personal information is the key to assessing and satisfying the GLBA compliance obligations.

(a) Personally identifiable financial information

The proposed NAIC and NCOIL model regulations both define "nonpublic personal information" as any "personally identifiable financial information," and any list or grouping

of consumers (and any publicly available information pertaining to them) that is derived using any personally identifiable financial information not available publicly. Conversely, “nonpublic personal information” does *not include* “publicly available information,” or any list derived without using any personally identifiable financial information not available publicly.

“Personally identifiable financial information” includes any information that a consumer provides or that is obtained in connection with a transaction involving a financial product or service and any list of names and addresses that is derived from such information. This term is expansive and includes, for example:

- (1) Information provided on loan, credit card or insurance applications;
- (2) Bank account or policy number information;
- (3) Information from a consumer report, and
- (4) Information collected through an Internet “cookie.”⁴

An example of a consumer list that is protected because it is developed from non-public personal information is a list of consumers’ names and street addresses derived in whole or in part using policy information, such as a list of customers who have purchased homeowners insurance. A consumer list that does not identify a specific consumer, such as aggregate information or blind data, without names, addresses or other nonpublic personally identifying information, however, would not be protected.

While these examples clarify what it means for information to be “personal,” there is another component to the definition – the information must not be “publicly available” to qualify for protection. The NAIC and NCOIL model acts and the federal privacy regulations all define “publicly available information” as any information that an agency has a reasonable basis to believe is lawfully available to the general public from:

- (1) Federal, State or local government records (such as government real estate records);
- (2) Widely distributed media (such as information from a telephone book, newspaper or publicly accessible web site); or
- (3) Disclosures to the general public that are required to be made by Federal, State or local law.

⁴ An Internet “cookie” is a tracking device that enables a web site to monitor a user’s web activities.

To ensure the reasonableness of a belief that information is publicly available, an agency should confirm that the information is of the type that is available to the general public, and take steps to determine if the consumer has sought to keep the information private. For example, an agency would have a reasonable basis to believe that mortgage information is publicly available if it determines that the information is of the type included on the public record where the mortgage is recorded. Likewise, an agency would have a reasonable basis to believe that an individual's phone number is publicly available if the phone number is listed.

(b) Personally identifiable health information

The GLBA does not specifically address the protection of health information. Thus, any health information that is collected in conjunction with selling or providing a financial service (including any insurance service) is treated by the GLBA as nonpublic financial information under the definition discussed above. There are several privacy regimes other than the GLBA, however, that regulate the way that health information may be handled. The particular health privacy requirements to which an agency will be subject vary depending on which of three groups a particular agency fits into.

The first group consists of agencies that do not sell health insurance but are exposed to health information in the course of selling financial products or services. Agents selling life or disability insurance fall into this group. This group is regulated by the GLBA which, as indicated above, simply treats health information that is collected in connection with providing a financial product as nonpublic financial information. The NAIC and NCOIL state privacy models, however, both include health information privacy provisions that would require agents and brokers to obtain affirmative authorizations from individuals before their nonpublic personal health information could be shared with any other party for marketing purposes (an "opt-in" right). An opt-in would be required essentially for all non-policy purposes.

The second group consists of agencies that sell health insurance products directly to individuals. This group will be regulated by the new HIPAA health privacy regulations. These regulations apply to health insurance agents and brokers and appear to supercede the proposed NAIC and NCOIL health privacy protections for recipients of individual health insurance policies and health benefit plans. The HIPAA regulations generally require:

- (1) The issuance of a separate set of privacy disclosures to individuals about whom protected health information is collected and/or disclosed;
- (2) The receipt of an affirmative "opt-in" authorization from an individual before protected health information may be used or disclosed (subject to a limited

number of exceptions);

- (3) Compliance with requests by individuals to provide access to their protected health information and to correct or amend this information, if necessary; and
- (4) Compliance with certain administrative requirements, such as designating a “privacy compliance officer” and an individual to handle all complaints and inquiries, and instituting policies and procedures designed to make sure that any protected health information that is disclosed is the “minimum necessary” to accomplish the purpose of the disclosure.

Appendix 12 addresses these obligations in more detail.

Finally, the third group consists of agents and brokers that sell *group* health insurance products and plans. This group also is subject to the HIPAA health privacy regulations, but its compliance with these regulations is significantly more complicated than the second group’s compliance. As such, it requires a more detailed analysis that is beyond the scope of this Guide.

In the meantime, agencies falling into both the second and third groups should note that persons and entities subject to the HIPAA rules have at least two years – until April 2003 – to comply with them. Agencies also should note that the Secretary of the Department of Health and Human Services, Tommy Thompson, has just officially reopened the HIPAA rules to another round of public comment. It is unclear at this stage what effect this will have on the HIPAA compliance requirements. As a final matter, agencies should note that the HIPAA rules set a “federal floor” of privacy protection for health information, which leaves open the door for States to enact health privacy requirements that are *more restrictive*. There are no current state laws that are more restrictive than the HIPAA regulations, and it is unclear whether any State will attempt to enact any such provisions.

B. THE GLBA PRIVACY NOTICE REQUIREMENT

The GLBA notice obligation requires all insurance agencies to provide an easily understandable notice of their privacy practices, including their basic handling of “nonpublic personal information,” to their “customers” when the customer relationship is established and on an at least annual basis thereafter. This notice obligation does not require agencies to engage in any specific information handling practices, only that they disclose the practices in which they do engage.

1. Who Must Receive A Privacy Notice?

Unless an insurance agency qualifies for the special agent exception discussed in Section I.A.1., it must provide a GLBA privacy notice to –

- (1) Any individual
- (2) Who purchases a financial product or service (including an insurance product or service) from or through that agency
- (3) That is to be used primarily for personal family or household purposes.⁵

These three elements describe individuals who are “customers.” As discussed in Part I.A.1, above, all customers are entitled to receive a GLBA privacy notice at the inception of the customer relationship.

In addition, a privacy notice must be provided to all “consumers”⁶ (anyone that has submitted personal information to the agency relating to a financial product or service) if the agency is going to share that information with a nonaffiliated entity for a non-exempted purpose.⁷ If the agency does not plan to share the personal information of these individuals (who are not customers because no customer relationship has been established) with a nonaffiliated third party for a non-exempted purpose, then the agency does not owe them a privacy notice.

2. What Must Be Included In The Notice?

As noted above, the GLBA does not require agencies to have any *particular* privacy policy in place (except for the opt-out requirement discussed below). Instead, an agency must disclose certain facts about its privacy policies. The disclosures must include the following:

- (1) The categories of nonpublic personal information that the agency collects (including the nature of the data collected and the means by which it is collected if the collection means are not obvious (such as by passive electronic monitoring)).
- (2) The categories of nonpublic information that may be disclosed.
- (3) The categories of affiliates and nonaffiliated third parties to whom such disclosures may be made, other than those to whom information is disclosed under an exception.⁸

5 The privacy notice obligations do not apply to companies or individuals that obtain products or services for business, commercial or agricultural purposes.

6 The GLBA uses the term “consumers” to refer collectively to all customers and all non-customers who have submitted personal information to a financial institution.

7 The privacy notice is provided to consumers in connection with an opt-out notification. The opt-out notification requirement is addressed in Part I.C.2, below.

8 See Part C, below.

- (4) The agency's policies and practices with respect to sharing nonpublic personal information about former customers. If an agency's policies are the same for customers and former customers, it may use the same clauses for both.
- (5) The categories of nonpublic personal information disclosed pursuant to agreements with third party service providers and joint marketers, and the categories of third parties providing the services (such as envelope stuffers).
- (6) The individual's right to opt-out of the disclosure of nonpublic personal information to nonaffiliated third parties.
- (7) Any disclosures regarding affiliate information sharing that the agency is providing under the FCRA.⁹
- (8) The agency's policies and practices with respect to protecting the confidentiality, integrity and quality of the nonpublic personal information it collects.

These disclosures must be "clear and conspicuous," which means that they must be "reasonably understandable" and "designed to call attention" to the nature and significance of the information in the disclosure. A notice is reasonably understandable if it uses short and clear explanatory sentences or bullet lists in plain language. A notice calls attention to the nature and significance of the information in it through the use of headings; easy-to-read type-styles; putting key words in boldface or italics; or shading or sidebars to draw attention to the notice when it is presented in combination with other information. A model notice that satisfies all applicable requirements is included in Appendix 1, and sample clauses that can be inserted into the model notice are included in Appendix 2.

3. When and How Should These Disclosures Be Made?

In general, an insurance agency's privacy policy must be disclosed initially when a "customer relationship" is established and on at least an annual basis thereafter. Agencies have three options for providing notice to their customers. They may:

- (1) Provide their own notice to the customer;
- (2) Provide a joint notice to the customer on behalf of both the agency and a carrier; or
- (3) Deliver the carrier's notice to the individual on the carrier's behalf.

Under all of these options, the initial notice can be provided when a purchased policy is delivered or when an agreement to provide other insurance services is consummated.

⁹ See Part II of this memorandum and Appendix 8.

The notice itself can be provided as part of or in conjunction with any other materials that an agency delivers to customers, including with the insurance contract or in an envelope with a bill for premiums.

The annual notice to customers also may be provided in these ways. Agencies should note that the GLBA does not require them to provide the annual privacy notice to a *former customer* – an individual with whom the institution no longer has a continuing relationship. Title insurance agents and other providers of real estate settlement services whose contact with the insured is limited to the time when the policy is sold are excused from the subsequent annual notice requirement after the initial notice is provided.

Finally, agencies that sell group insurance policies should note that the provision of their privacy notice to a plan sponsor (or group or blanket insurance policyholder) satisfies their notice obligations to plan participants (or individuals covered under the policy) as long as they do not disclose the participants' personal information to nonaffiliated entities other than as permitted under an exception. Similarly, an agency's obligations are satisfied by providing notice to a workers compensation plan participant and refraining from disclosing any protected information about that participant's beneficiaries to nonaffiliated third parties for non-exempted purposes.

C. THE GLBA OPT-OUT NOTICE REQUIREMENT

In addition to the privacy policy disclosure notice, before disclosing nonpublic personal information about any individual to a nonaffiliated third party for a non-exempted purpose, the agency must notify the consumer that the information may be shared and that he or she has a right to direct the agency not to disclose the information. This is known as a right to "opt-out" of the information sharing.

1. Who Must Comply?

In contrast to the privacy notice disclosure, which must be made regardless of whether information sharing takes place, the opt-out notification is required only if and when an agency intends *to disclose nonpublic personal information to a non-affiliated third party for a non-exempted purpose*.

The opt-out requirement applies only to information disclosures. If an agency does not share nonpublic personal information with other entities, or if a particular activity (such as cross-selling) does not warrant a disclosure, then the consumer is not owed an opt-out notification.

Moreover, the opt-out requirement applies only for disclosures to non-affiliated entities. If an agency shares discloses nonpublic personal information only to affiliated entities, the opt-out notification requirement does not apply. Thus, information sharing with

affiliates is permissible and consumers do not have a right to prevent it.

Finally, if an agency shares information with affiliates or nonaffiliated entities, but it does so only for exempted purposes, the opt-out notification requirement does not apply.

2. What Must Be Disclosed To Whom and When?

Under the opt-out requirement, an agency must inform its consumers that they have the right to prohibit the sharing of their nonpublic personal information with unaffiliated third parties for non-exempted purposes. The process of informing consumers of this right involves presenting consumers with an opt-out notice and giving them a reasonable opportunity to exercise their right to opt-out.

An example of an opt-out notice that satisfies the GLBA is provided in the sample privacy form in Appendix 3. There are a number of methods that can be used to offer consumers the opportunity to opt out. The methods that have been deemed reasonable under the GLBA are listed in the sample opt-out clause in Appendix 2 (See clause 3B). The methods include more traditional means of corresponding with consumers (such as mailing them an opt-out form on which they can check a box and sign and return the form to exercise their right to opt-out) as well as electronic methods (such as providing the notification through email or a web site). If an agency conducts business electronically and offers the opt-out electronically, the requirements of the Federal Electronic Signatures Act must be followed.¹⁰

A copy of the agency's privacy policy notice must be provided to consumers along with the opt-out notice. When providing an opt-out notice to consumers, however, agencies may choose to use a short-form privacy notice in lieu of their full privacy notice. A short form notice must state that the complete, long-form privacy notice is available on request; and it must give a reasonable means for obtaining the long form. For consumers with whom business is not conducted in person, a reasonable means includes providing a toll-free number that the consumer can call to request a copy of the full notice. For consumers with whom business is conducted in person, agencies should maintain copies of their long-form notice to provide immediately upon request. **Agencies may not use the short form notice option for customers. Customers always must receive the full privacy notice.**

3. What Is An "Affiliate"?

An affiliate is any entity that is under common ownership or common control with an agency's organization. The applicable regulations define common ownership to mean overlapping ownership of 25 percent or more. Hence, all subsidiaries of a parent company are

¹⁰ See Appendix 11.

affiliates of one another and of the parent. In addition, joint venture entities may be “affiliates” if one entity owns 25 percent or more of the joint venture or otherwise controls the affairs of the joint venture in any way.¹¹ The GLBA opt-out notice must be provided only if information is shared with non-affiliated third parties for a “non-exempted purpose.”

4. What are the “Exempted Purposes”?

There are several key exceptions to the opt-out notification requirement. If information is disclosed to a non-affiliated third party exclusively for one or more of the exempted purposes listed below, the opt-out notice is not required.

(a) Exception for processing and servicing transactions

A major exception to the opt-out right is that it does not prohibit an agency from sharing information for the purpose of processing or completing the insurance transaction (or a related transaction) for which the information was provided. Specifically, the opt-out requirements do not apply if a licensee discloses nonpublic personal financial information “necessary to effect, administer or enforce a transaction” that a consumer authorizes, or that takes place in connection with processing and servicing functions, including:

- (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 activities related to such a transaction.

“Necessary to effect, administer or enforce a transaction” includes disclosures: (i) necessary to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part; and (ii) necessary to underwrite insurance 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 pre-

¹¹ “Affiliate” is specifically defined as any company that is “related or affiliated by common ownership, or affiliated by corporate control or common corporate control, with another company.” This means controlling, controlled by, or under common control with, another company. “Control” means: ownership; the power to vote 25 percent or more of any class of voting securities; control over the election of a majority of the directors, trustees, or general partners;

mium payments, processing insurance claims, administering insurance benefits (including utilization review activities), and participating in research projects.

(b) Other limited exceptions

There are a few other limited exceptions to the opt-out requirement in the federal and proposed state regulations. Specifically, the opt-out requirements do not apply when an agency discloses nonpublic personal information:

- (1) With the consent or at the direction of the consumer (provided that the consumer has not revoked that consent);
- (2) To protect the confidentiality or security of the agency's records pertaining to the consumer, service, product or transactions, or to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability;
- (3) For required institutional risk control or for resolving consumer disputes or inquiries;
- (4) To persons holding a legal or beneficial interest relating to the consumer, or to persons acting in a fiduciary capacity on behalf of the consumer;
- (5) To provide information to insurance rate advisory organizations, guaranty funds, rating agencies, persons assessing an agency's compliance with industry standards, attorneys, accountants and auditors;
- (6) To a consumer reporting agency in accordance with the FCRA;
- (7) In connection with a proposed or actual sale, merger or transfer of a business or operating unit;
- (8) To the extent specifically permitted or required under other provisions of law, or to comply with Federal, State or local laws, rules and other requirements; and
- (9) To the extent that the NAIC or NCOIL model is applicable, for purposes related to the replacement of a group benefit plan, group health plan, group welfare plan, or workers compensation plan.

(c) Exception for service providers and certain marketing activities

The other primary exception to the opt-out requirement is for disclosures to nonaffiliated third parties for use by the third party to perform services for an agency or to engage in joint marketing activities with that agency. Such services include the marketing of the

institution's own products or services by an envelope stuffing service or other fulfillment service, or the marketing of financial products or services offered pursuant to a joint agreement between two or more financial institutions. A joint agreement means a written contract pursuant to which an agency and one or more financial institutions jointly offer, endorse or sponsor a "financial product" or service. **Independent property and casualty agents that are appointed by a number of insurance companies will in all likelihood want to enter into these joint agreements with each company for which they are appointed.** The exception for service providers and joint marketing activities is addressed in more detail in Appendix 4.

5. What If An Agency Revises Its Privacy Policy?

GLBA and the model regulations prohibit nonpublic personal information from being shared with a third party for a non-exempted purpose unless the consumer has been offered (and declined to exercise) the requisite opt-out right. If an agency revises its privacy policy to permit the sharing of information with a third party that was not identified as a potential recipient of the information for a purpose that was not identified, the nonpublic personal information cannot be shared with such a third party until the consumer has been notified of the revised policy and been given the requisite opportunity to opt-out.

6. Information Reuse and Redisclosure Limitations

If an agency receives nonpublic personal information from another nonaffiliated financial institution under a GLBA exception other than the joint marketing exception – e.g., as necessary to administer or complete a transaction at a consumer's request – its redisclosure and reuse of that information for marketing purposes is prohibited. Specifically, an agency may:

- (1) Disclose such information to the affiliates of a financial institution from which it received the information.
- (2) Disclose such information to its own affiliates, but the affiliates may use and disclose such information only to the extent that the agency would be able to do so.
- (3) Disclose such information pursuant to an exception **other than** the exception permitting disclosures for marketing purposes.

For example, if an agency receives a customer list from another financial institution for claims settlement purposes or in order to provide account processing services, it may disclose such information for fraud prevention or in response to a properly authorized subpoena. **It may not disclose such information, however, to a third party for marketing purposes or use that information for its own marketing purposes.** The same rule

applies, of course, to any third parties to whom the agency discloses protected information under an exception (other than for joint marketing).

This reuse/redisclosure limitation does not apply to information that is received from a nonaffiliated financial institution outside of an exception. For information that is received outside of an exception, any further disclosure of such information is governed by the same rules that would govern the disclosure of that information by the financial institution from which the information received. Thus, an agency could disclose such information to affiliates (the financial institution's or its own) or to any other person if the disclosure would be lawful if made by the financial institution from which the information was received.

D. DATA SECURITY AND INTEGRITY REQUIREMENT

All financial institutions that collect or maintain nonpublic personal information must institute mechanisms for protecting the security and integrity of that information. Security mechanisms are designed to protect the information from inadvertent disclosures. Integrity mechanisms, in contrast, are intended to protect nonpublic personal information that is maintained in an electronic medium from becoming corrupted. The rules do not, however, dictate that any specific mechanisms be instituted.

Appendix 10 includes an example of the types of safeguards that agencies are required to have in place to protect the security and integrity of customer records and information. Specifically, Appendix 10 contains the Standards for Safeguarding Customer Information that were issued by the federal banking agencies under the GLBA. While agencies may decide to follow these guidelines, they should know that they are not required to comply with these precise standards because they are not subject to the jurisdiction of the federal banking agencies.

PART II – THE FCRA AFFILIATE SHARING “OPT-OUT” REQUIREMENT

Compliance with the GLBA privacy obligations is not sufficient to meet obligations under other information-protecting laws, such as the federal Fair Credit Reporting Act. The key to understanding how the FCRA and GLBA fit together is knowing that they impose cumulative requirements, meaning that the more restrictive provisions apply.

The GLBA protects consumers from the disclosure of all nonpublic personal information to nonaffiliated third-parties for a non-exempted purpose.¹² It allows consumers to “opt-out” of such information-sharing with nonaffiliated entities. The GLBA does not, how-

¹² The FCRA imposes strict limitations on the sharing of personal “non-transactional” information with non-affiliated third parties for non-exempted purposes if the information is intended to be used for an insurance, credit or employment-related purpose. Because those limitations are not changed by the GLBA and because they do not include a disclosure component, they are not discussed here.

ever, apply to information sharing with affiliates.¹³ The FCRA protects a more limited category of information – “non-transaction” information used or expected to be used as a factor in establishing an individual’s eligibility for personal credit, insurance or employment. The FCRA allows consumers to “opt-out” of disclosures of such information before any such information can be shared with affiliates.

A shorthand way of understanding the key difference between the two statutes is knowing that the FCRA is concerned primarily with information that an agency receives **from** third parties (and passes on to its affiliates), whereas the GLBA is concerned primarily with information that an agency provides **to** third parties. For example, the FCRA requires that an opt-out right be provided before an agency can share with an affiliate any information that it gathers from a consumer’s credit report, such as credit history or credit scores, information on a motor vehicle report, or and any financial information that is provided on an insurance application. This information is treated as “non-transactional” information under the FCRA and this obligation therefore supercedes the less restrictive GLBA opt-out provisions.

In contrast, the FCRA does not impose any limitations whatsoever on the sharing of information about an agency’s direct experiences with the consumer. This type of “transaction” information includes, for example, information about the policies that the agency sold to the consumer, the consumer’s premium payment history, and the like. The GLBA “opt-out” notification obligation must be satisfied, however, before such information may be disclosed to a third party unless the disclosure is made for an exempted purpose.

Sample FCRA disclosure provisions are included in the Appendix 1 model privacy form. Finally, as noted above, Appendix 8 contains a separate memorandum that addresses the proposed FCRA regulations in greater detail.

CONCLUSION

As a practical matter, the most important first step an agency can take toward satisfying the GLBA privacy obligations is to develop a detailed policy for handling nonpublic personal information. This memorandum, the sample forms and clauses included in Appendices 1 – 4, and the privacy audit included in Appendix 13 are designed to assist with the development of that policy. In developing its privacy policy, an agency should remember that the disclosure of the policy may be treated as a contract between the agency and its clients. An agency should therefore take at least the following steps to make its policy a contract to which its customers have agreed.

¹³ The FCRA and the GLBA use the same definition of “affiliate” provided at footnote 11 to Part I.C.3.

- (1) An agency should consider including in its policy an alternative dispute resolution provision or arbitration clause that could help to reduce the costs of defending against potential challenges. An arbitration clause is included in the sample privacy form in Appendix 1.
- (2) An agency also should consider consolidating multiple privacy policies into a single disclosure form that it can utilize in all contexts in order to avoid conflicting obligations.¹⁴
- (3) An agency should institute quality assurance programs to ensure that each customer is given the requisite notice and that all other elements of its policies are maintained and followed at all times.
- (4) An agency should review its errors and omissions policies to ensure that they adequately address the new potential liabilities that failure to adhere to its own privacy policy may pose.

¹⁴ If an agency sells or administers group health/welfare plans and will be required to comply with the HIPAA health information privacy requirements, or if it intends to comply with the EU Safe Harbors, it may prefer to maintain two policies. These issues are discussed in more detail in the EU Privacy Directive memorandum in Appendix 9 and HIPAA memorandum in Appendix 12.