

# A FLORIDA AGENT'S GUIDE TO PRIVACY

Presented by

The Florida Association of Insurance Agents  
PO Box 12129  
Tallahassee, FL 32317-2129  
Telephone: 850-893-4155, Fax: 850-668-2852  
Web site: <http://www.faia.com>



June 2001

This guide is not intended to provide specific advice about individual legal, business, or other questions. It was prepared solely for use as a guide, and is not a recommendation that a particular course of action be followed. If specific legal or other expert advice is required or desired, the services of an appropriate, competent professional, such as an attorney, should be sought.

## **PREFACE**

The purpose of this guide is to enable Florida agents to comply with new privacy requirements mandated by the Gramm-Leach-Bliley Act (GLBA). That compliance must be in place by July 1, 2001, or agents may find themselves in violation of federal law.

In the near future, Florida will, by rule, adopt Florida-specific guidelines for compliance with the GLBA. FAIA will be working with the Department of Insurance (DOI) to assure that Florida's rules are consistent with and not more restrictive than the GLBA. To achieve as much uniformity as possible with other states, we will endeavor to base Florida's privacy rules on the National Association of Insurance Commissioners (NAIC) model regulation, already adopted in many jurisdictions. Florida does, however, already have in place laws regarding the use of information by banks and bank-associated agencies. Those current protections will remain in place and will not be superseded by DOI rules. When those new rules are adopted, we will update this package as needed. In the meantime, this guide will tell you what you need to do immediately if you are to be in compliance with the GLBA's privacy requirements.

*The Florida Association of Insurance Agents*

# PRIVACY ACTION STEPS

Each Florida agency should have a Privacy Action Plan in place by July 1, 2001. In order to facilitate your compliance, each agency should take the following action steps.

## ACTION STEP I

### Determine your current practice

1. Fill out the privacy audit on page 46. This will enable the agency to determine the current practice.
2. Determine the privacy policies of the carriers you represent.
3. Do you have any plans to change your practices in the near future?

## ACTION STEP II

### Develop plan to handle privacy notice requests

- A. Provide a copy of your privacy policy initially and annually thereafter to all customers regardless of your policy on sharing of information.
- B. If not sharing non-public personal information with unaffiliated third parties, beyond exceptions allowed by law:
  - ◆ No requirement to give privacy notice to “consumers” (prospective clients).
  - ◆ May be required by contract with carrier to deliver the carrier’s required notice.
- C. Public information can be shared regardless of notice. However, a “reasonable basis” test must be conducted to determine if it is in fact public information.
- D. If sharing non-public personal information for an exempt purpose:
  - ◆ A privacy notice is still required.
- E. If sharing a customer’s non-public personal information with non-affiliated parties for non-exempt purposes:
  - ◆ Initially when the customer (client) relationship is established.
  - ◆ Same notice to consumers (prospective clients) once they submit non-public personal information.
  - ◆ At least annually thereafter.
  - ◆ No requirement if it is a business customer.

- ◆ Additional notice of right to “opt out” (can be delivered at same time as policy notice).
- ◆ Sharing of health information with non-affiliates, beyond the allowed exceptions, requires “opt in” notice.
- ◆ If the privacy policy changes, all customers must be notified and given another opportunity to opt out.
- ◆ Individual’s notice and opportunity to opt out must be “clear and conspicuous”; i.e.: reasonably understandable and designed to call attention to their nature and significance.

### **ACTION STEP III**

#### **Other Issues**

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 on page 19.
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.
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 insurance policies to ensure that they adequately address the new potential liabilities that failure to adhere to its own privacy policy may pose.
5. Agency should keep records documenting their delivery of notice as well as the contents of their notice.
6. Regardless of any privacy notice requirements, each agency must meet the data security and confidentiality requirements of the GLBA.
7. Agencies that use web sites must make sure that their electronic privacy policy notice is in sync with their printed notice.

## **ACKNOWLEDGEMENTS**

In putting together this guide, we have borrowed heavily from the excellent materials supplied by the Independent Insurance Agents of America (IIAA) and Fireman's Fund Insurance Company. FAIA wishes to express its gratitude to both. Because of the comprehensive nature of the materials supplied by IIAA, we have included their [document](#) in its entirety on our web site. Also, we have reproduced several of their appendices in their entirety and made them part of this guide.

# TABLE OF CONTENTS

Preface .....	i
Privacy Action Steps .....	ii
Acknowledgements .....	iv
Table of Contents .....	v
The Gramm-Leach-Bliley Act (GLBA) .....	1
Who Must Comply? .....	2
Protected Information .....	3
How to Comply with Privacy Disclosure Notice .....	6
Opt-Out Requirements .....	9
Changes in Privacy Policy .....	12
Data Security and Integrity Requirements .....	13
Fair Credit Reporting Act .....	14
Conclusion .....	15
Appendix .....	17
Glossary of Terms .....	18
Sample Privacy Policy Notice .....	19
Privacy Policy Notice Clauses .....	23
Paragraph 1 Clauses .....	24
Paragraph 2 Clauses .....	25
Paragraph 3 Clauses .....	28
Paragraph 4 Clauses .....	31
Sample Opt-Out Form .....	33
Federal Banking Agencies Guidelines For Data Security .....	35
The Fair Credit Reporting Act and the FTC's Proposed Regulations ...	41
Internal Audit Questions .....	46
HIPAA Health Privacy Regulations .....	50
Florida DOI Informational Bulletin 00-004 .....	63

## **THE GRAMM-LEACH-BLILEY ACT (GLBA) AN OVERVIEW**

The Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act (GLBA) after its sponsors, was signed into law on November 12, 1999. It is the first comprehensive federal law governing the use of consumer information by financial institutions. Recognizing that Florida had long regulated the way banks and insurance interacted, in May of 1999, prior to the passage of GLBA, Florida enacted HB 897. That legislation was the culmination of three months of tough negotiations between agents' associations and the Florida Bankers Association. It embraced all of the consumer and agent protections contained in the 13 "safe harbors" of GLBA, and in some instances is even better than its federal counterpart. To the extent they are different than those in GLBA, the differences will be noted.

GLBA imposes three overarching privacy obligations on all "financial institutions." Insurance agents and agencies are specifically included within that definition. They must:

1. Provide a notice of the agency's non-public personal information handling practices;
2. Provide for an "opt out" right prior to information being shared with non-affiliated third parties for a non-exempted purpose; and
3. Institute data security and integrity mechanisms designed to protect non-public personal information.

The GLBA required federal regulators to promulgate regulations by November 13, 2000. These regulations were to protect the personal information provided to financial institutions and insurance companies by their consumers. The federal regulations have been delayed until July 1, 2001, and states were given the option of delaying implementation of their individual rules until that time. In Informational Bulletin 00-0004, issued on November 7, 2000, Florida's Department of Insurance opted for the delayed July 1, 2001, effective date (see appendix).

## **WHO MUST COMPLY?**

The GLBA's scope is very broad. It requires all insurance producers to comply with its privacy requirements unless they qualify for a specific exemption. Under the general terms of GLBA and under the provisions of the National Association of Insurance Commissioners' (NAIC's) model act upon which the Florida regulations will be based, there is an exemption that says insurance agents are not subject to the GLBA privacy notice requirements if they meet the following three specific conditions:

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

In other words, an insurance agency can be exempt from the notice requirements for any transaction on which it is acting as an agent for an insurance company and does not disclose any non-public personal information about that customer to any third party, except the insurance carrier or its affiliates, as long as the insurance company has itself complied with the notice requirements. Note, however, even if the agency does not have its own privacy policy and instead relies on the privacy policy of the carrier, the agency must still meet the data security and confidentiality provisions of the GLBA.

## PROTECTED INFORMATION

At the heart of the GLBA's privacy requirement is the protection of "non-public personal information" (NPI). Here we are basically talking about two types of information: (1) personally identifiable financial information; and (2) personally identifiable health information.

### Financial Information

It will aid in understanding the law to briefly explain each type, starting with personally identifiable financial information. It consists of 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 derived from such information.

The term is meant to be broad and includes, among other items, the following:

1. Information provided on loan, credit card, or insurance applications;
2. Bank accounts or policy number information;
3. Information from a consumer report or obtained from outside sources such as MVRs, credit reports, etc.;
4. Information collected through an internet "cookie;"
5. Lists 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; and
6. Obtained from knowledge of your "relationship" with the insured, such as how many years he has been with the agency, has he paid his bills in a timely manner, etc.

To be protected, the information must be personally identifiable financial information not available publicly. To put it another way, it does not include "publicly available" information. Examples of "publicly available" information, and thus exempt, include:

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 assessable web site); or
3. Disclosures to the general public that are required to be made by federal, state, or local law.

Note, however, to ensure the reasonableness of a belief that the information is publicly available, an agent must confirm that (a) the information is of a type that is available to the general public and (b) the consumer has not taken steps to keep the information private. An example may be useful. Normally, an individual's telephone number would be publicly available. However, if that person has an unlisted telephone number, it may be classified as non-public personal information.

### Health Information

The second type of information an agent needs to consider is personally identifiable health information. While GLBA does not specifically address the protection of health information, it may be indirectly covered. Since health care information is not usually publicly available, any such information collected in conjunction with selling or providing financial services, such as insurance, is treated as non-public financial information under GLBA and is probably of a protected class.

In addition to that, there are other sources that also regulate the way health information is handled. Which laws apply is, in large part, a factor of how your agency obtains the information. There are three general groups of agents affected.

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 and services. Agents selling life or disability insurance are in this group. Under GLBA, this information is treated like any other non-public financial information and triggers the three-part process of notice, opt-out rights and security and integrity protection of data (to be discussed later). However, the NAIC privacy model upon which Florida's new regulation will be based requires an opt-in right—agents and brokers would have to obtain affirmative authorization from the individual before their non-public personal health information could be shared with any other person for marketing purposes. In effect, an opt-in would be required for all non-policy purposes.

The second group consists of agencies that sell health insurance products directly to individuals. In this case, the general provisions of GLBA are overridden by the more specific requirements of the Federal Health Insurance Portability and Accountability Act (HIPAA). The HIPAA regulations generally require:

1. The issuance of a separate set of privacy disclosures to individuals about when 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). A sample opt-in form is supplied in IIAA's Guide to Privacy appendix.

3. Compliance with requests by individuals to provide access to their protected health information and to correct or amend this information if necessary.
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 to make sure the protected health information that is disclosed is the "minimum necessary" to accomplish the purposes of the disclosure.

The third group to consider consists of agents and brokers who sell group health insurance products and plans (as distinguished from group two, who sells individual health plans). This group is also subject to HIPAA health privacy regulations, but its compliance with these regulations is more complicated than the second group's compliance. As such, it requires more detailed analysis that is beyond the scope of this guide. It is also subject to change since the HIPAA rules are being rewritten.

Fortunately, agencies falling into both the second and third group have until April 2003 to comply with the ultimate HIPAA rules. Note, however, the HIPAA rules set a "federal floor," or minimum level, of privacy protection for health information and Florida's privacy rules may end up being more restrictive than HIPAA's. The Florida rules also may have an earlier effective date, although this is not being considered at this time.

## HOW TO COMPLY WITH PRIVACY DISCLOSURE NOTICE

Once you have determined that your activities do not totally exempt you from compliance, the next step is to determine how to comply with the privacy disclosure notice requirement. To address that, we need to break the question down into four parts:

1. Who must receive the privacy notice?
2. What must be included in the notice?
3. When must the notice be made?
4. How should the privacy disclosure be made?

Think of it as who, what, when and how.

### WHO?

Who must receive the privacy notice? Those who are defined as “customers.” A “consumer” is anyone who purchases or seeks to purchase a financial product or service for personal, family or household use. A customer relationship starts when the consumer is issued a policy. A customer, therefore, includes:

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

By definition, this means that the privacy notice obligations do not apply to companies or individuals that obtain products or services for business, commercial or agricultural purposes. While it makes a difference whether the individual is a “customer” or a “consumer,” that will be discussed later. “Customers” must receive notice; “consumers” may not always need notice.

Note: Under NAIC’s definition of “customer,” you will find workers’ compensation policyholders. Under NAIC’s definition of “consumer,” you will find insurance claimants. The NAIC model has not yet been adopted in Florida.

### WHAT?

What must be included in the notice? The GLBA does not dictate the specific type of privacy policy that the agency must adopt. Instead, GLBA provides an agency need only disclose the following facts in its privacy policy:

1. The categories of non-public 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 non-public information that may be disclosed.
3. The categories of affiliates and non-affiliated third parties to whom such disclosures may be made, other than those to whom information is disclosed under an exception.
4. The agency's policies and practices with respect to sharing non-public 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 non-public 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 non-public personal information to non-affiliated third parties.
7. Any disclosures regarding affiliate information sharing that the agency is providing under the Fair Credit Reporting Act (FCRA).
8. The agency's policies and practices with respect to protecting the confidentiality, integrity and quality of the non-public personal information it collects.

These disclosures must be "clear and conspicuous" (i.e. reasonably understandable and designed to "call attention to both their nature and significance"). A notice is reasonably understandable if it uses short and clear explanatory sentences or bullet lists in plain language. A notice calls attention to its nature and significance through the use of headings, easy-to-use type styles, putting keywords in bold face or italics, or using shading or sidebars to draw attention to the notice. Model language and sample clauses to modify the model are contained in the Appendix.

#### WHEN?

When should the notices be provided? The answer to this depends on whether you are dealing with a "customer" or "consumer." As was pointed out on page 6, a "customer" is an individual who purchases an insurance product or service that is to be used primarily for personal family or household purposes. A "consumer," on the other hand, is anyone who has submitted personal information to the agency relating to a financial product or service, but is not yet and never becomes a customer.

For a "customer," the insurance agency's privacy policy must be disclosed

- ◆ Initially when the customer relationship is established; and
- ◆ At least annually thereafter.

The initial notice must be provided to all customers by July 1, 2001. It can be provided to those becoming customers when the purchased policy is delivered or when an agreement to provide other insurance services is consummated. An annual notice is required to all customers thereafter. Note, there is no requirement that the agency provide annual privacy notice to a former customer.

For a “consumer,” there is an annual notice requirement, but only if the agency is going to share that information with a non-affiliated entity for a non-exempt purpose. **If the agency does not plan to share the personal information of these “consumers” (i.e. individuals who are not customers because no customer relationship has been established), then the agency does not owe them a privacy notice.**

#### HOW?

How should the privacy disclosure be made? Once it has been established that disclosure should be made, agencies have three options for doing so. 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.

The notice can be made:

1. In a stand-alone mailing;
2. As part of, or in conjunction with, other materials an agency delivers to the customer;
3. In an envelope with the bill for the premium; or
4. Handed to the customer in person.

Special rules apply for group insurance. Agencies that sell group insurance should know that the provisions in their privacy notice that is given to the plan sponsor also satisfies their notice obligations to the plan participants, as long as they do not disclose the participants' personal information to non-affiliated entities (other than as permitted under an exception).

Special rules also apply to agencies transferring data from the European Union. This, too, is complex and beyond the scope of this guide. If you deal in such information, see the excellent discussion in Appendix IX of IIAA's Guide to Privacy.

Finally, agencies that do business over the Internet and that will be satisfying the privacy requirements using electronic means may come under the provisions of the Electronic Signatures and Global and National Commerce Act. If your agency falls into that category, see Appendix XI of IIAA's Guide to Privacy for further discussion.

## OPT-OUT REQUIREMENTS

In addition to the privacy policy disclosure notice which must be made regardless of whether information sharing takes place, GLBA provides for an opt-out requirement that must be met before disclosing NPI about an individual to a non-affiliated third party for a non-exempt purpose. In those cases, the agency must tell the customer that the agency intends to share the NPI and must give the consumer a chance to say no, or opt-out. A sample opt-out form is contained in the appendix.

The best way to address this provision is to look at (1) who must comply, and (2) what must be disclosed, to whom, and when?

Who must comply with the opt-out requirements?

There is a two-part test. The opt-out notification is required only if and when an agency intends to disclose NPI:

1. To a non-affiliated party
2. For a non-exempt purpose.

An “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.” That is defined to mean as having overlapping ownership of 25 percent or more. Therefore, all subsidiaries of a parent company are affiliates of one another and of the parent. In addition, joint ventures 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. Since that is the definition of “affiliated,” then everything else is non-affiliated!

An “exempt purpose” is the second half of the test. If information is disclosed to a non-affiliated third party exclusively for one or more exempted purposes, then the opt-out notice is not required. Under GLBA, there are three classes of exempted purposes:

- A. The exception for processing and servicing transactions. This covers disclosure “necessary to effect, administer or enforce a transaction” that a customer authorizes, or that takes place in connection with processing and servicing functions. They include:
  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...” includes

1. 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
2. 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 premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), and participating in research projects.

B. A second set of exemptions to the opt-out requirement includes disclosure of NPI:

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 models are applicable, for purposes related to the replacement of a group benefit plan, group health plan, group welfare plan, or workers' compensation plan.
- C. The final set of exemptions from the opt-out requirements is for disclosures to non-affiliated 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 marketing 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. According to IIAA, independent property and casualty agents who are appointed by a number of insurance companies should enter into these joint agreements with each company for which they are appointed if the agency and the insurance company engage in joint marketing activities to offer, endorse or sponsor a financial product of service. However, some experts believe that there is no need for a joint marketing agreement between a carrier and its appointed agent. Those experts suggest that joint marketing agreements are for other unrelated activities, such as those between an agent and a bank.

## CHANGES IN PRIVACY POLICY

What happens if you send the opt-out information and the customer declines to opt-out but you later expand the scope of those with whom you will share the information? In that case, GLBA requires you to send a new opt-out notice listing the expanded distribution before you share the information with additional non-affiliates.

### Information you receive from others

If an agency receives non-public personal information from another non-affiliated 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 re-disclosure and reuse of that information for marketing purposes is prohibited. However, an agency may:

1. Disclose such information to the affiliates of the non-affiliated 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 joint 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.** If you obtain information from another financial institution outside of an exception, you can disclose it to affiliated parties of the financial institution that gave it to you. You can also give it to your own affiliates but they can only use it to the extent that you could. Finally, information you obtain from another financial institution can only be used by you to the extent the financial institution could have used it.

## **DATA SECURITY AND INTEGRITY REQUIREMENTS**

Setting aside for a moment all of the discussions about exceptions and exclusions, all financial institutions, including insurance agencies, that collect or maintain NPI must institute mechanisms for protecting both the security and integrity of that information. The difference between the two is that security mechanisms are designed to protect the NPI from disclosure, whereas the integrity mechanisms are designed primarily to protect electronically stored data from becoming corrupted. However, the security and integrity requirements apply to both electronic and hard-copy data. While there are no specific mechanisms required by GLBA, some guidance can be found by looking at what banks are required to do under their regulations (see the appendix for a comprehensive discussion).

## **FAIR CREDIT REPORTING ACT**

Compliance with the GLBA privacy obligations is not necessarily 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 non-public personal information to nonaffiliated third parties for non-exempted purposes. It allows consumers to opt-out of such information sharing with non-affiliated entities. The GLBA does not, however, apply to information sharing with affiliates. 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, and/or 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 model privacy form in the appendix. Finally, as noted above, the appendices contain a separate memorandum that addresses the proposed FCRA regulations in greater detail.

## **CONCLUSION**

The Gramm-Leach-Bliley Act places new privacy provisions on information collected by agents. The GLBA goes into affect on July 1, 2001, in Florida and this guide is designed to assist agents in coming into compliance with the provisions of the GLBA. Additionally, because of the overlap of regulation, three other laws—FCRA, HIPAA, and the European Union's regulations—impact privacy requirements. To the extent they may impact your agency, you should be familiar with their provisions.

To fully understand your responsibilities under these various regulatory provisions, we would recommend the following:

1. Carefully read this guide and its appendices (including IIAA's Guide to Privacy);
2. Answer the questions contained in the Privacy Audit;
3. Develop a privacy policy for your agency; and
4. Prepare your agency's Privacy Policy Notice and Privacy "Opt-out" Form from the attached samples and send them to your customers in an appropriate and timely manner.

Additionally, the agency should consider taking the following steps in developing its privacy policy:

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 the appendix.
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. Note, however, that 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 IX and HIPAA memorandum in Appendix XII of the accompanying guide to privacy produced by IIAA.
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 develop procedures to assure data security and data integrity.
5. An agency should review its E&O insurance policies to ensure that they adequately address the new potential liabilities that failure to adhere to its own privacy policy may pose.
6. An agency needs to understand and comply with the privacy laws of other states and countries in which it does business.

This guide and the additional materials from IIAA should assist you in coming into compliance with the current federal privacy requirements.

As we go to press, Florida's Department of Insurance (DOI) is in the process of developing its own set of privacy rules. They will be based on the NAIC model regulations and be consistent with and no more restrictive than those of the GLBA. We will update this guide as soon as those Florida-specific rules are final.

**APPENDIX**

Glossary of Terms ..... 18

Sample Privacy Policy Notice ..... 19

Privacy Policy Notice Clauses ..... 23

    Paragraph 1 Clauses ..... 24

    Paragraph 2 Clauses ..... 25

    Paragraph 3 Clauses ..... 28

    Paragraph 4 Clauses ..... 31

Sample Opt-Out Form ..... 33

Federal Banking Agencies Guidelines For Data Security..... 35

The Fair Credit Reporting Act and the FTC's Proposed Regulations ..... 41

Internal Audit Questions ..... 46

HIPAA Health Privacy Regulations ..... 50

Florida DOI Informational Bulletin 00-004 ..... 63

## GLOSSARY OF TERMS

*Affiliate:* Any company that is “related or affiliated by common ownership, or affiliated by corporate control or common corporate control, with another company.” That is defined to mean as having overlapping ownership of 25 percent or more. Therefore, all subsidiaries of a parent company are affiliates of one another and of the parent. In addition, joint ventures 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. Everything else is a non-affiliate.

*Consumer:* An individual who has submitted personal information to the agency relating to a financial product or service, but who has not purchased the product or service and is, thus, not yet a customer. In other words, a customer relationship has not yet been established.

*Cookie:* Computer files that contain information created by a web server that can be stored on the user’s hard disk for use either during a particular session (“pre-session” cookie) or for future use (“persistent” cookie).

*Customer:* An individual who establishes a long-term relationship by purchasing an insurance product or service that is to be used primarily for personal, family or household purposes.

*FCRA:* Fair Credit Reporting Act

*GLBA:* Gramm-Leach-Bliley Act

*HIPAA:* Health Insurance Portability and Accountability Act and the December 28, 2000, rules issued by the Department of Health and Human Services.

*Joint Marketing Agreement:* A written contract pursuant to which an agency and one or more financial institutions jointly offer, endorse or sponsor a “financial” product or service.

*NPI:* Non-public personal information.

## **SAMPLE PRIVACY POLICY NOTICE**

This section will assist in the creation of a privacy policy notice that will convey to customers your agency's practices for collecting and sharing nonpublic information. Use the sample clauses from the section beginning on page 23 to develop a privacy notice that accurately reflects the type of information you collect and the type of parties that the information is disclosed.

**[Insert name of institution]**  
**Privacy Policy Notice**  
(as of [insert date])

**PURPOSE OF THIS NOTICE**

Title V of the Gramm-Leach-Bliley Act (GLBA) generally prohibits any financial institution, directly or through its affiliates, from sharing nonpublic personal information about you with a non-affiliated third party unless the institution provides you with a notice of its privacy policies and practices, such as the type of information that it collects about you and the categories of persons or entities to whom it may be disclosed. In compliance with the GLBA, we are providing you with this document, which notifies you of the privacy policies and practices of [insert name of institution].

[If you share with third-parties for a non-exempted purpose, insert the following:] [The GLBA further requires that we inform you that you have a right to prevent us from sharing nonpublic personal information about you with a non-affiliated third party for any purpose that is not specifically authorized by law. Your right to prevent us from sharing nonpublic personal information about you with a non-affiliated third party for a purpose that is not specifically authorized by law is called your right to “opt out” of such information sharing.]

**OUR PRIVACY POLICIES AND PRACTICES**

**1. Information we collect:**

[Insert clause 1(a) or 1(b) from the list on page 24 labeled “Paragraph 1 Clauses,” depending on which one applies to you.]

**2. Information we may disclose to third parties:**

[Insert clause 2(a), 2(b), 2(c), 2(d), 2(e), 2(f) or 2(g) from the list on pages 25–27, labeled “Paragraph 2 Clauses,” depending on which best describes your disclosure practices.]

**3. Nonaffiliated third parties to whom disclosures may be made:****A. Nonaffiliated Third Parties To Whom Disclosures May Be Made**

*[Insert clause 3A(1), 3A(2), 3A(3) or 3A(4) from the list on pages 28–30, labeled “Paragraph 3A Clauses,” depending on which best describes your disclosure practices.]*

**B. Notification of Your Right To Opt Out of Certain Disclosures**

*[If you disclose information to non-affiliated third parties other than as permitted by an express GLBA exception, Insert clause 3B from the list on Page 30, labeled “Paragraph 3B Clauses.” (If you do not disclose information to non-affiliated third parties other than as permitted by an express GLBA exception, then you are not required to provide this opt out notification on your privacy form.)]*

**4. Affiliates with whom we share certain information protected by the Fair Credit Reporting Act, unless you tell us not to:**

*[If you have affiliates with whom you share non-transactional, FCRA-protected information, insert the three Fair Credit Reporting Act clauses contained in “Paragraph 4 Clauses” on pages 31–32. If you do not have affiliates with whom you share such information, then you can delete paragraph 4 entirely from your privacy notice and should renumber the paragraphs below.]*

**5. Our practices regarding information confidentiality and security:**

We restrict access to nonpublic personal information about you to those employees who need to know that information in order to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

**6. Our policy regarding dispute resolution:**

Any controversy or claim arising out of or relating to our privacy policy, or the breach thereof, shall be settled by arbitration in accordance with the rules of the American Arbitration Association, and judgment upon the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

**7. Reservation of the right to disclose information in unforeseen circumstances:**

In connection with the potential sale or transfer of its interests, [*insert name of institution*] and its affiliates [*if any*] reserves the right to sell or transfer your information (including but not limited to your address, name, age, sex, zip code, state and country of residency and other information that you provide through other communications) to a third party entity that (1) concentrates its business in a similar practice or service; (2) agrees to be [*name of institution*]'s successor in interest with regard to the maintenance and protection of the information collected; and (3) agrees to the obligations of this privacy statement.

**8. Changes to our Policy:**

If we revise our procedure relating to this privacy policy, we will provide notice of the changes.

**9. Customer acknowledgement and signature:**

By signing my name below, I am indicating that I have read the privacy policy of [*insert name of institution*] and that I understand its terms. No promises or representations have been made to me to induce me to sign this form.

---

Customer Signature

Date

If you have any questions about this notice, please contact us at [*insert phone number or other contact information*] during normal business hours.

## **PRIVACY POLICY NOTICE CLAUSES**

This section contains sample clauses for use in satisfying your GLBA privacy notice disclosure obligations. These clauses are referred to in the sample privacy form on page 19. Where you have a choice of clauses that depends on the particular practices of your company, the sample form directs you to these clauses, and you should select the clause that applies to you. The numbered paragraphs of the sample form on page correspond to the sections in this section. Thus, where you must choose a clause on the sample form to complete Paragraph 2, you will look in this section for the page that lists “Paragraph 2 Clauses.”

**PRIVACY POLICY NOTICE – PARAGRAPH 1 CLAUSES**

**The following clauses are used to describe the categories of information that you collect about your consumers.**

1(a) *[If you collect information about your consumers:]*

We collect nonpublic personal information about you from the following sources *[insert all that apply]*:

- ◆ Information we receive from you on applications or other forms.
- ◆ Information about your transactions with us, our affiliates or others.
- ◆ Information we receive from a consumer reporting agency.
- ◆ *[Insert any other categories of information that you collect]*

Unless it is specifically stated otherwise in an amended Privacy Policy Notice, no additional types of information will be collected about you.

1(b) *[If you do not collect any information:]*

We do not collect any information about you.

## **PRIVACY POLICY NOTICE – PARAGRAPH 2 CLAUSES**

**The following clauses are used to describe the categories of information that you disclose to third parties (affiliates or non-affiliates). The information in italics at the beginning of each choice tells you the circumstances in which each clause applies.**

- 2(a) *[If you disclose nonpublic personal information outside a stated exception, and you disclose all of the categories of information that you collect:]*

We may disclose all of the information that we collect about you, as described above.

- 2(b) *[If you disclose nonpublic personal information outside a stated exception, but you only disclose some categories but not others:]*

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

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

- 2(c) *[If you do not disclose nonpublic personal information outside of a stated exception, other than the exception for service providers and joint marketing:]*

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.<sup>1</sup>

We share nonpublic personal information with our own affiliates.<sup>2</sup>

---

1 **Note to agents:** This language assumes that you treat your customers and former customers the same. If you do not, you must include **two separate disclosure paragraphs**, one describing your practices for customers and one describing them for former customers. This is true for every paragraph in your privacy notice that describes practices that differs for customers and former customers. Thus, anytime you see a description in these clauses that groups “customers and former customers” together, you should decide whether that language is true for your company. If it is not true, then you must include separate statements.

2 This clause is not needed if you do not share NPI with affiliates.

- 2(d) *[If you disclose information under the service provider/joint marketing exception, and you disclose all of the categories of information that you collect:]*

We may disclose all of the information we collect, as described above, about our customers or former customers, to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

- 2(e) *[If you disclose information under the service provider/joint marketing exception, but you disclose only some categories of information and not others:]*

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

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

- 2(f) *[If you disclose information under both the service provider/joint marketing exception and one or more other stated exceptions, and you disclose all of the categories of information that you collect:]*

We may disclose all of the information we collect, as described above, about our customers or former customers, to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements. We also may disclose information about our customers or former customers as permitted by law.

- 2(g) *[If you disclose information under both the service provider/joint marketing exception and one or more other stated exceptions, but you disclose only some categories of information and not others:]*

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

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

We also may disclose information about our customers or former customers as permitted by law.

### **PRIVACY POLICY NOTICE – PARAGRAPH 3 CLAUSES**

The following clauses are used to describe the categories of third parties to whom you disclose nonpublic personal information. The information in italics at the beginning of each choice tells you the circumstances in which each clause applies.

3A(1) *[If you disclose nonpublic personal information to non-affiliated entities outside of a stated exception:]*

We may disclose nonpublic personal information about you to the following types of third parties, unless you tell us not to:

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

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

3A(2) *[If you do not disclose nonpublic personal information to non-affiliated entities outside of a stated exception, **other than** the service provider/joint marketing exception:]*

We disclose nonpublic personal information about you only to non-affiliated third parties as permitted by law.

3A(3) *[If you disclose information to non-affiliated entities under the service provider/joint marketing exception:]*

We may disclose nonpublic personal information about you, such as we have described above, to the following types of third parties that perform marketing services on our behalf or with whom we have joint marketing agreements:

- ◆ Fulfillment service providers, such as *[provide illustrative examples, such as “envelope stuffing services”]*;
- ◆ Financial institutions with whom we have joint marketing agreements, such as *[provide illustrative examples, such as (include all that apply to you)]*:
  - ◆ *national banks and their subsidiaries;*
  - ◆ *Federal branches and Federal agencies of foreign banks,*

- and any subsidiaries of such entities;*
- ◆ *member banks of the Federal Reserve System;*
  - ◆ *branches and agencies of foreign banks and commercial lending companies owned by foreign banks;*
  - ◆ *organizations operating under the Federal Reserve Act;*
  - ◆ *bank holding companies and their non-bank subsidiaries;*
  - ◆ *banks insured by the FDIC;*
  - ◆ *insured state branches of foreign banks and any subsidiaries of such entities;*
  - ◆ *savings associations, the deposits of which are insured by the FDIC, and any subsidiaries of such savings associations;*
  - ◆ *federally insured credit unions and any subsidiaries thereof;*
  - ◆ *securities brokers or dealers;*
  - ◆ *investment companies; and*
  - ◆ *insurance providers]*
  - ◆ We do share nonpublic personal information with our own affiliates.<sup>3</sup>

3A(4) *[If you disclose information to non-affiliated entities under **both** the service provider/joint marketing exception and one or more other stated exceptions:]*

We may disclose nonpublic personal information about you, such as we have described above, to the following types of third parties that perform marketing services on our behalf or with whom we have joint marketing agreements:

- ◆ Fulfillment service providers, such as *[provide illustrative examples, such as “envelope stuffing services”]*;
- ◆ Financial institutions with whom we have joint marketing agreements, such as *[provide illustrative examples, such as the following (include any or all that apply to you):*
  - ◆ *national banks and their subsidiaries;*
  - ◆ *Federal branches and Federal agencies of foreign banks, and any subsidiaries of such entities;*
  - ◆ *member banks of the Federal Reserve System;*
  - ◆ *branches and agencies of foreign banks and commercial lending companies owned by foreign banks;*
  - ◆ *organizations operating under the Federal Reserve Act;*
  - ◆ *bank holding companies and their non-bank subsidiaries;*
  - ◆ *banks insured by the FDIC;*

---

<sup>3</sup> This clause is not needed if you do not share NPI with affiliates.

- ◆ *insured state branches of foreign banks and any subsidiaries of such entities;*
- ◆ *savings associations, the deposits of which are insured by the FDIC, and any subsidiaries of such savings associations;*
- ◆ *federally insured credit unions and any subsidiaries thereof;*
- ◆ *securities brokers or dealers;*
- ◆ *investment companies; and*
- ◆ *insurance providers]*

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

**The following clause describes the right to opt out of certain information sharing with non-affiliated third parties.**

3B As we have indicated in this Privacy Policy Notice, we collect certain nonpublic personal information about you, and we may disclose that information to certain non-affiliated third parties for purposes other than those expressly permitted by the Gramm-Leach-Bliley Act and the federal and state regulations implementing that Act. If you prefer that we not disclose nonpublic personal information about you to non-affiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than those disclosures that are expressly permitted by the Gramm- Leach-Bliley Act and its implementing regulations).

If you wish to opt out of such disclosures to non-affiliated third parties, you may: [*insert one or more of the following reasonable means of opting out:*

- ◆ *Call us toll free at (insert toll free number); or*
- ◆ *Visit our website at (insert web site address) and (provide further instructions on how to use the web site option);<sup>4</sup> or*
- ◆ *E-mail us at (insert the e-mail address); or*
- ◆ *Fill out and tear off the bottom of this sheet and mail it back to the to the address shown there; or*
- ◆ *Check the appropriate box below or on the attached form (insert a box with text next to it that says "I wish to opt out," or refer to the **SAMPLE OPT-OUT FORM** on pages 33 and 34)].*

---

4 **Note to agents on electronic means of opting out:** If you use a website or an e-mail address as the only means by which a consumer may opt out, the consumer must agree to the electronic delivery of information. What this means is that, if you are currently transacting business with consumers on line, you may provide them with their opt out notifications electronically, as long as the requirements of the federal electronic signatures act are met. \*\*\* describes the requirements of the federal electronic signatures act. **If you are not currently transacting business with your consumers online, however,** it is problematic for you to offer them the opportunity to opt out only via electronic means unless you get clear permission in advance from such consumers stating that they agree to the electronic delivery of information.

### **PRIVACY POLICY NOTICE – PARAGRAPH 4 CLAUSES**

The following clauses are used to describe the required disclosures under the Fair Credit Reporting Act. If you share non-transactional information with your affiliates, you must insert the following three clauses [all three are required] into your privacy form, as directed in paragraph 4 of the sample privacy form (pages 19–22).

- A. Information we can share with our affiliates, unless you tell us not to:  
Unless you tell us not to, we may share with our affiliated companies information about you, including:
- ◆ Information we obtain from your insurance application, such as your income or your marital status;
  - ◆ Information we obtain from a consumer report, such your credit score or credit history;
  - ◆ Information we obtain to verify representations made by you, such as your open lines of credit; and
  - ◆ Information we obtain from a person regarding its employment, credit, or other relationship with you, such as your employment history.
- B. Our affiliated companies who may receive this information are:
- ◆ Financial service providers, such as:  
*[insert your financial affiliates – you can describe them by name or by category, such as “mortgage lenders and brokers”]*
  - ◆ Non-financial companies, such as:  
*[insert your non-financial affiliates – you can describe them by name or by category, such as retailers, direct marketers, airlines, and publishers]*
  - ◆ Our other affiliates, such as:  
*[name any other affiliates or describe them by category, such as “non-profit organizations”]*

C. How to tell us not to share this information with our affiliated companies:

If you prefer that we not share this information with our affiliated companies, you may direct us not to share this information by doing the following:

*[insert one or more of the following reasonable means of opting out:<sup>5</sup>*

- ◆ *Call us toll free at (insert toll free number); or*
- ◆ *Visit our web site at (insert web site address) and (provide further instructions on how to use the web site option);<sup>6</sup> or*
- ◆ *E-mail us at (insert the e-mail address); or*
- ◆ *Fill out and tear off the bottom of this sheet and mail it back to the to the address shown there; or*
- ◆ *Check the appropriate box on the attached form (insert a box with text next to it that says "I wish to opt out," or refer to the **SAMPLE OPT-OUT FORM** on pages 33–34)]*

Note: Neither the GLBA nor the NAIC model regulation requires this clause. However, many financial institutions are doing it anyway.

---

5 **Note to agents on combining opt out forms under the FCRA and GLBA:** The opt out methods listed here are the same methods of opting out permitted under the GLBA. You may allow consumers to exercise both opt out rights on the same form, or you can issue two separate forms. For example, you can issue one form with two boxes – one that has text next to it saying "I want to exercise my right under the FCRA to opt out of affiliate information sharing" and one that has text saying "I want to exercise my right under the GLBA to opt out of information sharing with non-affiliated third parties."

6 **Note to agents on electronic means of opting out:** If you use a website or an e-mail address as the only means by which a consumer may opt out, the consumer must agree to the electronic delivery of information. What this means is that, if you are currently transacting business with consumers on line, you may provide them with their opt out notifications electronically, as long as the requirements of the federal electronic signatures act are met. See IIAA's Privacy Kit for a description of the requirements of the federal electronic signatures act. **If you are not currently transacting business with your consumers online, however,** it is problematic for you to offer them the opportunity to opt out only via electronic means unless you get clear permission in advance from such consumers stating that they agree to the electronic delivery of information.

## **SAMPLE OPT-OUT FORM**

This section is an example of an opt out form that you can give to customers in person to exercise their right to opt out of certain GLBA information sharing. It is an example of just one method by which you can offer the opportunity to opt out (other methods are described in the opt out notice clauses that appear on pages 23–32, specifically in clauses 3B and 4C). This particular form combines the GLBA opt out and FCRA opt out on the same form. If you are required to offer both the GLBA and the FCRA opt out notification, you can use same form, as we have done here, or you can use two different forms.

**[Insert name of institution]**  
**Opt Out Form**  
(as of [insert date])

Please read the text below and decide whether you wish to exercise your right to opt out of the information sharing described. If you choose to exercise your right to opt out, you must mail this form back to us at [insert address]. Your response must be postmarked no later than 30 days from the date you received this notice from us in person in order for it to be valid. If you do not mail this form back or do not mail it back within 30 days, you have not exercised your opt out right, and we can share the information described.

\_\_\_\_\_ I wish to exercise my right under the Gramm-Leach-Bliley Act to opt out of [insert name of institution]'s sharing nonpublic personal information about me to non-affiliated third parties [and affiliates<sup>7</sup>] for purposes other than those that are permitted by law.

\_\_\_\_\_ I wish to exercise my right under the Fair Credit Reporting Act to opt out of [insert name of institution]'s sharing nontransactional information about me to affiliates.

\_\_\_\_\_  
Customer Signature

\_\_\_\_\_  
Date

<sup>7</sup> The phrase "and affiliates" is not necessary if you are not providing the affiliate opt-out.

## **FEDERAL BANKING AGENCIES GUIDELINES FOR DATA SECURITY**

This section provides an example of the types of data security and integrity safeguards that must be implemented and followed under GLBA. Agencies are not required to implement these precise standards, but they provide a good example of the type of safeguards required under GLBA.

## Federal Banking Agencies Joint Guidelines For Establishing Standards For Safeguarding Customer Information

While the Gramm-Leach-Bliley Act (GLBA) requires that you establish data security and integrity safeguards, the GLBA does not specify precise safeguards or guidelines. In order to help agents and brokers address these requirements, this appendix provides the "Inter-agency Guidelines Establishing Standards for Safeguarding Customer Information" **as an example** of the type of safeguards that you must implement and follow under the GLBA.

These Guidelines were issued by the federal banking agencies as a joint final rule.<sup>8</sup> The regulations are reproduced here in memorandum form to make them easier to review. Specifically, we have chosen to reproduce the version of these Guidelines issued by the Federal Reserve System. While you are not required to implement these precise standards, because you are not subject to the jurisdiction of the Board (or any of the federal banking agencies), they nevertheless provide a good example of the type of safeguards that the GLBA requires.

---

### I. Introduction

These Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines) set forth standards pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 and 6805). These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

#### A. Scope

The Guidelines apply to customer information maintained by or on behalf of bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisors), for which the Federal Reserve Board (the Board) has supervisory authority.

#### B. Preservation of Existing Authority

These Guidelines do not in any way limit the authority of the Board to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices. The Board may take action under these Guidelines independently of, in conjunction with, or in addition to, any other enforcement action available to the Board.

---

8 66 Fed. Reg. 8616 (Feb. 1, 2001).

**C. Definitions**

- (1) Except as modified in the Guidelines, or unless the context otherwise requires, the terms used in these Guidelines have the same meanings as set forth in sections 3 and 39 of the Federal Deposit Insurance Act (12 U.S.C. §§ 1813 and 1831p-1).
- (2) For purposes of the Guidelines, the following definitions apply:
  - (a) Board of directors, in the case of a branch or agency of a foreign bank, means the managing official in charge of the branch or agency.
  - (b) Customer means any customer of the bank holding company as defined in 216.3(h) of this chapter.
  - (c) Customer information means any record containing nonpublic personal information, as defined in 216.3(n) of this chapter, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the bank holding company.
  - (d) Customer information systems means any methods used to access, collect, store, use, transmit, protect, or dispose of customer information.
  - (e) Service provider means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank holding company.
  - (f) Subsidiary means any company controlled by a bank holding company, except a broker, dealer, person providing insurance, investment company, investment advisor, insured depository institution, or subsidiary of an insured depository institution.

**II. Standards for Safeguarding Customer Information****A. Information Security Program**

Each bank holding company shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank holding company and the nature and scope of its activities. While all parts of the bank holding company are not required to implement a uniform set of policies, all elements of the information security program must be coordinated. A bank holding company also shall ensure that each of its subsidiaries is subject to a comprehensive information security program. The bank holding company may fulfill this requirement either by including a subsidiary within the scope of the bank holding company's comprehensive information security program or by causing the subsidiary to implement a separate comprehensive information security program in accordance with the standards and procedures in sections II and III of this appendix that apply to bank holding companies.

**B. Objectives**

A bank holding company's information security program shall be designed to:

- (1) Ensure the security and confidentiality of customer information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

**III. Development and Implementation of Information Security Program****A. Involve the Board of Directors**

The board of directors or an appropriate committee of the board of each bank holding company shall:

- (1) Approve the bank holding company's written information security program; and
- (2) Oversee the development, implementation, and maintenance of the bank holding company's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

**B. Assess Risk**

Each bank holding company shall:

- (1) Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
- (2) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
- (3) Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

**C. Manage and Control Risk**

Each bank holding company shall:

- (1) Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank holding company's activities. Each bank holding company must consider whether the following security measures are appropriate for the bank holding company and, if so, adopt those measures the bank holding company concludes are appropriate:
  - (a) Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent em-

- employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.
- (b) Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
  - (c) Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
  - (d) Procedures designed to ensure that customer information system modifications are consistent with the bank holding company's information security program;
  - (e) Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;
  - (f) Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
  - (g) Response programs that specify actions to be taken when the bank holding company suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
  - (h) Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.
- (2) Train staff to implement the bank holding company's information security program.
  - (3) Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank holding company's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

#### ***D. Oversee Service Provider Arrangements***

Each bank holding company shall:

- (1) Exercise appropriate due diligence in selecting its service providers;
- (2) Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and
- (3) Where indicated by the bank holding company's risk assessment, monitor its service providers to confirm that they have satisfied their

obligations as required by paragraph D(2). As part of this monitoring, a bank holding company should review audits, summaries of test results, or other equivalent evaluations of its service providers.

**E. Adjust the Program**

Each bank holding company shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank holding company's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

**F. Report to the Board**

Each bank holding company shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank holding company's compliance with these Guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

**G. Implement the Standards**

- (1) *Effective date.* Each bank holding company must implement an information security program pursuant to these Guidelines by July 1, 2001.
- (2) *Two-year grandfathering of agreements with service providers.* Until July 1, 2003, a contract that a bank holding company has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of section III (D), even if the contract does not include a requirement that the servicer maintain the security and confidentiality of customer information, as long as the bank holding company entered into the contract on or before March 5, 2001.

## **THE FAIR CREDIT REPORTING ACT AND THE FTC'S PROPOSED REGULATIONS**

This section provides an overview of the Federal Trade Commission (FTC) proposed interpretations of the Fair Credit Reporting Act (FCRA) as it relates to the handling of information. This section describes the manner in which institutions can communicate information about consumers to affiliates of the institution without incurring the obligations of consumer reporting agencies.

## The Fair Credit Reporting Act and the FTC's Proposed Regulations

In December 2000, the Federal Trade Commission (FTC) issued proposed interpretations of the Fair Credit Reporting Act (FCRA)<sup>9</sup> that permit institutions to communicate information about consumers<sup>10</sup> to affiliates<sup>11</sup> of the institutions (affiliate information sharing) without incurring the obligations of consumer reporting agencies. The proposed regulations authorize institutions to communicate among their affiliates two categories of consumer information:

- (1) "Transaction or Experience Information," which may be communicated to affiliates without restrictions; and
- (2) "Opt Out Information," which may be communicated to affiliates provided that certain conditions are met.<sup>12</sup>

Although the proposed regulations do not define transaction or experience information, they clarify the difference between such information and "opt out information" by giving examples of categories of information that qualify as opt out information. The general approach is consistent with requiring that the customer be provided with an opt out before insurance information submitted in conjunction with credit applications may be shared with affiliates; however, that express example is not included in the regulations.

The significant provisions of the proposed regulations are discussed below.

### **Consumer Report**

The touchstone of the FCRA affiliate information-sharing restrictions is its definition of "consumer report." In general, the term means any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit, insurance or employment purposes.

---

9 Unless otherwise noted, all citations are to 65 Fed. Reg. 80,806- 80,809 (Dec. 18, 2000), where the FTC's proposed "Commentary on the Amended Fair Credit Reporting Act (Affiliate Information Sharing)" is set forth.

10 "Consumer" is defined simply as "an individual."

11 "Affiliate" is 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.

12 The proposed regulations explain that both types of information are covered by the FCRA, but there are restrictions imposed on the sharing of opt out information with affiliates that are not imposed on the sharing of transaction or experience information with affiliates.

Among other things, the following categories of information are specifically excluded from the definition of “consumer report”:

- (1) Any report containing information solely as to transactions or experiences between the consumer and the person making the report;
- (2) Any communication of that information among affiliates;
- (3) Any communication among affiliates of opt out information as long as certain conditions are satisfied.

### ***Transaction or Experience Information***

The proposed rule tracks the statutory language of the FCRA referring to “transaction or experience information” but, like the statute, does not specifically define that term.

### ***Opt Out Information***

The proposed FCRA rules use the term “opt out information” to refer to information that is protected by the FCRA but that is not transaction or experience information. The proposed rule defines opt out information as information that:

- (1) Bears upon a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living;
- (2) Is used or expected to be used or collected to serve as a factor in establishing the consumer’s eligibility for credit or for another of the permissible purposes listed in the FCRA (e.g., credit transactions, insurance underwriting, employment purposes); and
- (3) Is not a report containing information solely as to transactions or experiences between the consumer and the person reporting or communicating the information.

Additional guidance is provided in the proposed regulation that governs the contents of an opt out notice, where categories of information that qualify as opt out information are provided.

### ***Communication of Opt Out Information to Affiliates***

The proposed regulations provide that an institution’s communication to its affiliates of opt out information about a consumer is not a “consumer report” if the following conditions are met:

- (1) The institution has provided the consumer with an opt out notice;
- (2) The institution has given the consumer a reasonable opportunity and means, before it communicates the information to its affiliates, to opt out; and
- (3) The consumer has not opted out.

### **Contents of Opt Out Notice**

In general, an opt out- notice must be clear and conspicuous and must explain the categories of opt out information about an institution's consumers that the institution communicates to its affiliates, the categories of affiliates to which is communicates such information, the consumer's right to opt out, and a reasonable means for opting-out.

An institution satisfies the requirement to categorize the opt out information that it communicates if it lists the following categories of information (as applicable) along with examples to illustrate the type of information in each category. Those categories include:

- (1) Information from a consumer's application;
- (2) Information from a consumer's credit report;
- (3) Information obtained by verifying representations made by a consumer; or
- (4) Information provided by another person regarding its employment, credit or other relationship with a consumer.

Examples of information within one of these categories would include, e.g., a consumer's:

- (1) Income
- (2) Credit score or credit history with others;
- (3) Open lines of credit with others;
- (4) Employment history with others;
- (5) Marital status; and
- (6) Medical history.

### **Coordination with Privacy Regulations**

If a financial institution is required to provide FCRA disclosures and an opt out notice under the FCRA, those notices must be included in the initial and annual privacy notice mandated by the GLBA. The cover memorandum and sample privacy form included as Appendix I demonstrate how to provide the requisite FCRA disclosures.

Clear and conspicuous. Like the GLBA rules, the proposed FCRA rule requires that notices be "clear and conspicuous," which is defined to mean reasonably understandable and designed to call attention to the nature and significance of the information it contains. Although the proposed regulations do not mandate the use of any particular technique for making a notice clear and conspicuous, they offer a detailed list of examples of what constitutes "reasonably understandable" (e.g., uses bullet lists and every day words, and avoids multiple negatives) and what constitutes "designed to call attention" (e.g., uses easy-to-read typeface, and boldface or italics for key words). This list is the same as the one used in the GLBA regulations.

Reasonable opportunity to opt out. The proposed rule provides that, in general, an institution provides a reasonable opportunity to opt out if it provides a reasonable period of time following the delivery of the opt out notice for the consumer to opt out. Examples of a reasonable period of time in which to opt out are:

- (1) 30 days from the date of delivery in person of an opt out notice;
- (2) 30 days from the date of mailing an opt out notice
- (3) 30 days from the date a consumer acknowledges receipt of an electronic notice.

You should refer to the Insurance Agent and Broker's Guide to Privacy and the sample privacy form and notice clauses for a demonstration of how to implement the FCRA regulations and how to coordinate your obligations under the FCRA with your obligations under the GLBA.

## **INTERNAL AUDIT QUESTIONS**

This section contains questions that will assist you in reviewing your information handling practices and in developing a privacy policy that meets the requirements of GLBA. Use this section to determine the types of information that your agency collects and discloses as well as any data security and integrity procedures you may already have in place.

## INTERNAL AUDIT QUESTIONS

In order to develop your privacy policy, you will need to communicate with all of your organization's divisions to determine what nonpublic personal information is being collected, for what purpose, and with whom it is being shared. These questions are intended to guide you in reviewing your information handling practices and in developing a privacy policy that is consistent with your obligations under the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act.

### **General Business Questions**

1. Which employees have access to nonpublic personal information?
2. Do these employees understand the privacy issues outlined in the Insurance Agent and Broker's Guide to Privacy?
3. Are procedures in place to educate employees on any privacy issues that they do not understand?
4. Is privacy a subject covered in employee training?
5. Are procedures in place to deal with privacy issues, events and concerns as they develop?

### **General Information Handling Questions**

6. What categories or kinds of information do you collect?
7. What are the mechanisms you use for collecting this data?
8. What person or entity collects it?
9. For what purpose(s) is it collected?
10. Is data that is collected for one purpose is ever used for another purpose?

### **Questions Relating to Information Security and Integrity**

11. What mechanisms do you use to protect the safety, confidentiality and integrity of the information you collect?
12. What mechanisms do you use to prevent unauthorized access or use of the information?
13. Do you have a list of every employee or type of employee who will have access to personal data?
14. Which of these employees actually need access to such information in order to carry out their assignments?
15. Do your employees that have access to such information understand the importance of reporting security glitches or other problems relating to preserving the confidentiality and integrity of the information you collect?

**Disclosure of Information to Third Parties<sup>13</sup>**

16. Do you disclose nonpublic personal information to affiliates or non-affiliated entities? If so, you must answer the following questions (questions 17-22).
17. What are the categories or kinds of information that you disclose to third parties?
18. What are the categories of persons or entities to whom you disclose nonpublic information (including both affiliates and non-affiliated third parties)?
19. What are the purposes for which the data is disclosed?
20. Is the information collected about former customers treated the same way?
21. If not, how is its treatment different?
22. Who are your employees that deal with third parties? (You should inform all of your employees who deal with third parties of the importance of reporting any suspected misuses of shared information as soon as possible).

**Information Disclosure to Non-Affiliated Third Parties<sup>14</sup>**

23. Do you disclose nonpublic personal information to non-affiliated third parties? If so, you must answer the following questions (questions 24-30)
24. Is the third party's use of the information limited solely to providing services on your behalf?
25. If so, what kind of services?
26. Does the third party's usage fit within a category specifically exempted by the GLBA?
27. If so, what category or categories (see attached cover memorandum for a list of specific exemptions, such as servicing and processing transactions)?
28. Do you share information with non-affiliated parties for purposes of jointly marketing financial products, or with service providers (such as envelope stuffers) to market your own products?
29. Do you have contracts in place with the persons or entities to whom you disclose nonpublic information for marketing purposes?
30. Are there specific limitations in those contracts on how the information can be used?

**Questions Relating to the GLBA Opt Out Right<sup>15</sup>**

31. Do you share GLBA information with unaffiliated third parties for purposes other than those specifically permitted by the GLBA? If so, you will need to provide an opt out notification, and you should answer the following questions (questions 32-33).
32. Do you have mechanisms in place that will allow data to be separated if the opt out right is exercised?

---

13 You will use the information gathered here to assist you in selecting appropriate clauses to satisfy paragraph 2 of the sample privacy form on pages 19–22. For example, the clauses from which you may choose to satisfy paragraph 2 (see pages 23–32) ask you to list the kinds of information you may disclose to third parties (see Clause 2(b) on page 25). Your answers here will assist you in listing such categories of information.

14 You will use the information gathered here to assist you in selecting clauses to satisfy both paragraphs 2 and 3 of the sample privacy form on page 19. For example, you must determine whether the disclosures you are making are covered by a GLBA exception in order to select a number of the clauses listed for paragraphs 2 and 3 (such as the clauses numbered 2(e) or 3A(2) on pages 23–32).

15 Your answers here will assist you in determining whether you have to make the GLBA opt out disclosure in paragraph 3B of the sample privacy form on pages 19–22.

33. Do you have mechanisms in place that will allow to you confirm whether the opt out right has been exercised?

**Questions Relating to the FCRA Opt Out Right**<sup>16</sup>

34. Do you have affiliates with whom you share nontransactional information? If so, you must answer the following questions (questions 35-39).
35. What type of nontransactional information do you share with your affiliates?
36. For what purposes is it shared?
37. Does the information you share with your affiliates bear upon consumer credit worthiness, credit standing, credit capacity, character, general reputation, or mode of living?
38. Is the information that you share used to as a factor in establishing a consumer's eligibility for credit, insurance or employment purposes?
39. If you answer questions 37 and 38 in the affirmative, you are required to provide your consumers with an opportunity to opt out of your sharing such information with affiliates.

**Handling Complaints and Inquiries**

40. How are your policies regarding the collection, use and distribution of information explained to your customers?
41. Who is in charge of handling consumer complaints and inquiries?
42. How are consumer complaints and inquiries handled?
43. Are complaints and inquiries logged?
44. Is there a commitment to correcting errors?
45. Are there mechanisms in place to resolve consumer disputes if they arise?

**Transfer of Personal Data from Members of the European Union**

46. Do you transfer personal data from European Union member states?
47. If so, then you should refer to Appendix IX of IIAA's Guide to Privacy and comply with the requirements listed therein.

**Reviewing Vendor Contracts**

48. Do you transfer nonpublic personal information to third parties pursuant to service provider or vendor contracts or pursuant to joint marketing agreements?
49. If so, you should obtain copies of all contracts or agreements and review them for compliance with the GLBA service provider/joint marketing exception. (To ensure compliance with the exception, you will need to make sure that the contracts have certain language prohibiting the third party from reusing or redisclosing such information other than as permitted by law. You should refer to IIAA's Guide to Privacy for more information about the service provider/joint marketing exception and sample contract language.)

---

<sup>16</sup> Your answers here will assist you in determining whether you have to make the FCRA disclosures in paragraph 4 of the sample privacy form on pages 19–22.

## **HIPAA HEALTH PRIVACY REGULATIONS**

This section addresses privacy obligations under HIPAA for agents selling health insurance policies directly to individuals. Agents selling health insurance policies (including long term care policies) should insert into their privacy policy the proper sample clauses in this section to ensure compliance with the HIPAA privacy regulations.

## INTRODUCTION

On December 28, 2000, the Department of Health and Human Services (HHS) issued its Health Insurance Portability and Accountability Act (HIPAA) rules governing the protection of “individually identifiable health information.” The rules protect all medical records and other individually identifiable health information held or disclosed by health insurance agencies and other “covered entities” and their “business associates.” Compliance with these regulations is required by February 26, 2003. While HHS has indicated that it may reconsider certain aspects of these rules, it is not expected that such reconsideration will substantively alter any of the requirements outlined here.

This section contains two parts. *Part I* provides an analysis of the new health privacy regulations as applied to insurance agents that sell health insurance policies directly to individuals and that share protected health information solely for purposes of selling or servicing such policies. It does not address the more complicated rules that govern sharing health information for other purposes or that govern group health plans.

*Part II* contains clauses that agencies selling health insurance policies to individuals may insert into their GLBA privacy notice to help ensure that their notices also comply with HIPAA. While compliance with HIPAA is not mandated for another two years, we are offering these clauses so that you can develop one privacy policy that complies with both the GLBA and HIPAA at the same time. The proposed clauses in Part II are sufficient to the extent that you are: (1) selling health insurance policies to individuals; and (2) sharing these individuals' health information solely for purposes relating to selling and/or servicing those policies. If you sell group health insurance or share health information for any other purpose, different rules apply that are not addressed here.

## PART I – ANALYSIS

### A. Who and What is Covered by the New HIPAA Rules?

#### 1. The HIPAA Regulations Apply To Health Insurance Agents

The regulations generally apply to “health plans,” “health care clearinghouses” and most “health care providers” – categories collectively referred to as “covered entities.” The compliance requirements also apply to “business associates” that receive or are exposed to individually identifiable health information in the course of providing services for covered entities. Insurance agents and brokers that sell health insurance policies (including long term care policies) are “covered entities” subject to the HIPAA requirements. When agents are engaged in activities on behalf of health insurers, they are deemed “business associates” of those insurers under the rules.

#### 2. The HIPAA Regulations Do Not Apply To Many Types of Policies

Several types of insurance benefits are exempt from regulation. *This means that personal information gathered in the course of offering these benefits is not subject to the compli-*

*ance requirements.* Excepted benefits include workers' compensation, life, disability, property and casualty, and automobile insurance. Reinsurers also are exempted; however, a covered entity's performance of reinsurance-related activities (such as handling reinsurance payments for a self-insured plan) is governed by the rules.

The rules recognize that one entity may perform both covered and non-covered functions. For example, an agent may sell both health insurance and workers' compensation insurance. Only the information gathered in connection with the sale of health insurance is subject to the requirements of the rules. The covered entity owes a privacy notice to health plan enrollees but not to enrollees in the excepted benefit plan. (The notice requirement is described below.)

That said, an agency that performs both covered and non-covered functions must keep these functions separate. In terms of record-keeping, this means that the agency must prevent protected health information from being mixed with unprotected information and later being handled in a way that violates the rules. The agency also must establish policies and procedures to ensure that any part of its workforce that is performing mixed functions does not impermissibly use or disclose protected health information.

### **3. The Rules Protect All Forms of Individually Identifiable Health Information**

The HIPAA rules protect all medical records and other "individually identifiable health information" held or disclosed by certain entities *in any form* – whether communicated electronically, on paper or in oral conversations. Individually identifiable health information is a subset of personal information, including demographic information, collected from an individual. Specifically, it is health information that satisfies the following three conditions:

- (1) The information is created or received by a health care provider, health plan (including a health insurance issuer or agent), employer, or health care clearinghouse;
- (2) The information relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- (3) The information either identifies the individual or provides a reasonable basis for believing that it can be used to identify the individual.

#### **B. HIPAA Compliance Requirements**

The HIPAA health privacy rules impose four sets of compliance requirements on "covered entities" such as agents selling health insurance directly to individuals. These are (1) notice requirements; (2) "opt in" requirements; (3) access requirements; and (4) administrative requirements.

## 1. **Notice Requirements**

Covered entities must maintain a privacy policy and generally are required to provide notice of such policy to recipients of health care and health insurance benefits. The notice content requirements are similar (but not identical) to those imposed under the GLBA.

### (a) Content of Notice

Like the GLBA regulations, the HIPAA rules contain a notice requirement for covered entities. In general, an individual has a right to receive notice of the uses and disclosures of protected health information that may be made by the covered entity, and of such individual's rights and the covered entity's duties with respect to protected health information. A covered entity's use and disclosure of protected health information must be consistent with its privacy notice.

A HIPAA notice must include certain specific statements or clauses. These required HIPAA statements may be combined with a GLBA notice. In Part II, a list of clauses that can be added to the sample GLBA notice in Appendix I to make it HIPAA compliant is provided. These clauses are sufficient if an agency sells health policies directly to individuals and *only shares* protected health information for purposes relating to servicing those policies. If an agency shares protected health information for other purposes (such as marketing), it cannot rely only on these clauses. These clauses also are inadequate to the extent an agency sells or services group policies or plans. For either, additional disclosures not addressed in this section will be necessary.

### (b) When to Provide Notice

The HIPAA notice must be provided to all health insurance insureds by February 2003. Thereafter, the notice must be provided whenever a policy is purchased.

There also are two ongoing notice requirements. Notice must be provided within sixty days of any revisions to the privacy policy. Additionally, once every three years, the covered entity must remind health insureds of the availability of the privacy notice and how to obtain it. The notice rules differ – both in terms of content and in terms of who must provide notice – for group health plan arrangements.

## 2. **“Opt In” Requirements**

In order to use or disclose protected health information, an agency either must obtain affirmative permission from the individual (an “opt in”) or determine that no opt in is required. As a general matter, insurance agencies are not required to obtain an “opt in” to use or disclose protected information for “treatment, payment or health care operations” provided that they:

- (1) Are selling (or servicing) health insurance policies directly to (or for) individuals, and
- (2) Have satisfied the “business associate” requirements discussed below.

An opt in is required to use or disclose such information for any other purpose (such as marketing).

(a) “Treatment, Payment, and Health Care Operations”

For covered entities other than health care providers, no opt in is required for “treatment, payment and health care operations” provided they otherwise comply with the rules. Treatment means the provision, coordination or management of health care by a health care provider. For insurance agents and brokers, the activities that constitute “payment” and “health care operations” are more relevant.

“Payment” refers to activities undertaken by a covered entity (or its business associate) to determine or fulfill its responsibility for coverage and provision of benefits, or to obtain or provide reimbursement for the provision of health care. Examples of payment activities include, but are not limited to:

- (1) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
- (2) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- (3) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
- (4) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- (5) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
- (6) Disclosure to consumer reporting agencies of certain categories of protected health information relating to collection of premiums or reimbursement, including name, address, date of birth, social security number, payment history, and account number.

“Health care operations” include a broad range of insurance-related activities, including the use of protected information maintained by a entity for that entity’s underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care.

(b) When an Opt In Is Required?

An “opt in” is required whenever a covered entity (or its business associate) uses and/or discloses protected information for purposes *other than* performing functions that constitute “treatment, payment or health care operations.” For example, an opt in is required to use or disclose protected information for most marketing communications; to place a contract for excepted benefits; and to obtain protected information from other covered entities for purposes of pre-enrollment underwriting.

There are three narrow marketing situations, however, in which an authorization is not required. These three situations arise when the marketing communication:

- (1) Occurs in a face-to-face encounter with an individual;
- (2) Concerns products or services of nominal value; or
- (3) Concerns health-related products or services of the covered entity or a third party.

If the communication fits within one of these categories, no authorization is required as long as the covered entity:

- (1) Clearly identifies itself as the party making the communication;
- (2) Prominently states whether it is being compensated for the communication; and
- (3) Describes how the individual may opt out of receiving future such communications (unless the communication is included in a broadly disseminated document, such as a newsletter).

The suggested compliance clauses included in Part II, below; are based on the assumption that you *do not share health information for marketing purposes*.

(c) Required Elements for a Valid Opt In Authorization

An authorization cannot be combined in the same document with a privacy notice. In general, two authorizations may be contained in the same document, but documents that create compound or confusing authorizations are prohibited.

An authorization must use specific language to describe the purpose for which the authorization is sought. All authorizations must contain the following *core elements*:

- (1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- (2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- (3) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

- (4) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
- (5) A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
- (6) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;
- (7) Signature of the individual and date.

Additional elements are required depending on what type of authorization the covered entity requests. If an agency requests an authorization for its *own* use or disclosure of protected health information (*e.g.*, for marketing purpose), the authorization also must contain the following elements:

- (1) Where applicable, a statement that the agency will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;
- (2) A description of each purpose of the requested use or disclosure;
- (3) A statement that the individual may inspect or copy the protected health information in accordance with the access requirements;
- (4) A statement that the individual may refuse to sign the authorization
- (5) If use or disclosure of the requested information will result in direct or indirect remuneration to the agency from a third party, a statement that such remuneration will result.

If an agency requests an authorization to disclose information to third parties, the authorization must include the core elements as well as the following:

- (1) A description of each purpose of the requested disclosure;
- (2) Except for an authorization on which payment may be conditioned, a statement that the agency will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure; and
- (3) A statement that the individual may refuse to sign the authorization.

### **3. Access Requirements**

A covered entity must permit individuals access to inspect and amend their protected health information. If the entity does not possess the information, it must inform the individual of where to direct the request. In addition, individuals generally have a right to receive a written "accounting of disclosures" of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested. An accounting of disclosures is not required, however, for disclosures made to carry out treatment, payment and health care operations.

### **4. Administrative Requirements**

Covered entities must designate both a privacy compliance officer and an individual to receive and respond to complaints and inquiries about the entity's privacy policies and practices. A covered entity also must implement policies and procedures to enable it to verify the identity of the individual or entity requesting protected information, and to ensure that the information that is disclosed is the "minimum amount necessary" to carry out the purpose for which the information was requested.

## **C. Health Insurance Agents Are Business Associates of the Insurance Carriers Whose Policies They Sell to Individuals**

The rules governing "business associates" do not displace the compliance rules generally applicable to covered entities. They simply enable certain persons ("business associates") to perform functions for covered entities without requiring any permission from the individual. They also permit a covered entity (such as a health insurance carrier) and its business associate (such as a health insurance agent) to use or disclose protected information under a single opt in.

### **1. What is a Business Associate?**

A "business associate" is a person or entity that performs certain activities or functions on behalf of a covered entity (other than as the member of the workforce) that involve the use or disclosure of protected health information. Such functions may include claims processing and claims administration, benefit management, repricing or other functions regulated by the rules. Other functions include carrying out "payment" and "health care operations," which brings a wide range of insurance-related activities performed by the agent on behalf of the carrier (including placing or renewing an insurance contract, underwriting, premium rating, and collecting premiums) within the scope of the business associate rules. Depending on the particular relationship between an agent and health insurance carrier, an agent may perform any or all of these functions on behalf of the carrier. Thus, agents are business associates of the health insurance carriers whose insurance they sell.

The regulations include a narrow exception to the business associate definition for "conduits." Generally, any organization through which health information passes without that organization ever accessing the information is not considered a business associate. For example, the U.S. Postal Service is a conduit and not a business associate. Similarly, financial institutions that process consumer-conducted debits, credits, or electronic fund

transfers are also considered to be conduits of personal health information and not business associates. Although this exception generally does not apply to agents selling health insurance directly to individuals, we do not rule out the possibility that there may be some situations in which an agent acts purely as a conduit. In such a case, the business associate rules would not apply.

## **2. *Business Associate Rules Do Not Affect An Agency's Compliance with the Notice, Access and Administrative Requirements***

HIPAA's business associate rules do not affect the notice, access and administrative requirements. Thus, health insurance agencies and health insurance carriers generally are required to provide and maintain their own privacy policy notices and to satisfy the access and administrative requirements discussed above.

There is one exception. If an agent and a health insurance carrier are legally separate entities but subject to common ownership and control,<sup>14</sup> they may designate themselves as "affiliated covered entities" for purposes of compliance. Affiliated covered entity status would entitle them to comply with the rules as if they were a single legal entity. For example, affiliated covered entities need to provide and maintain only one privacy policy notice. Only if they are affiliated covered entities will the rules permit an agent and a health insurance carrier to provide and maintain the same privacy policy notice.

## **3. *No Opt In is Necessary for Disclosures of Protected Health Information Between the Agent and Carrier or by the Agent on Behalf of the Carrier as Long as a Business Associate Contract is In Place***

The business associate rules permit covered entities to disclose protected information to business associates and they permit business associates to create or receive such information on their behalf without obtaining an opt in. Before such disclosures can be made, however, the rules require that covered entities and their business associates have a "business associate contract" in place to satisfactorily assure that the business associate will appropriately safeguard the information. These contracts must define the boundaries of permissible use or disclosure of protected information by the business associate. Furthermore, a business associate contract may not authorize the business associate to use or further disclose protected information in any manner that would violate the rules if done by the covered entity.

---

<sup>14</sup> Common control exists if an entity has the power to influence or direct the actions or policies of another entity. Common ownership exists if an entity or entities possess an ownership or equity interest of **5 percent** or more in another entity.

(a) Business Associate Contracts – Required Elements

In terms of content, a business associate contract must include provisions stating that the business associate will:

- (1) Not use or further disclose the information other than as permitted by the contract or required by law;<sup>15</sup>
- (2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
- (3) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
- (4) Ensure that any subcontractors to whom it provides protected health information agree to the same restrictions and conditions that apply to the business associate;
- (5) Make protected health information available in accordance with the access requirements.
- (6) Make its internal practices, books, and records relating to the use and disclosure of the protected health information available to the Secretary for purposes of determining the covered entity's compliance; and
- (7) At the termination of the business associate contract, if feasible, return or destroy all protected health information.

The contract also must authorize termination by the covered entity if the covered entity determines that the business associate has violated a material term of the contract. A covered entity violates the rules if it has *actual knowledge* of a pattern or practice of the business associate that constitutes a material breach or violation of the associate's obligation under the contract, unless the covered entity takes reasonable steps to cure the breach or end the violation.

(b) Effect of Valid Business Associate Contract

With a valid business associate contract in place, a covered entity may disclose protected information to a business associate and permit the associate to create or receive protected information on its behalf without obtaining permission from the individual. This rule insulates the carrier and agent with respect to disclosures *between or on behalf of each other*, but it does not displace any other rule. Thus, before it permits the agent to use, disclose or collect such information, the carrier first must determine the purpose for which the information will be used and whether or not an opt in is required for that purpose. If an

---

<sup>15</sup> There are two exceptions. The contract may permit the business associate to: (1) use and disclose protected information for the proper management and administration of the business associate, and (2) provide data aggregation services relating to the health care operations of the covered entity. Data aggregation is defined as a service that involves combining personal health information data from more than one covered entity, for the purpose of data analysis that relates to the health care operations of the covered entities being serviced.

opt in is required, the agent may be the person to obtain the opt in (on the carrier's behalf) because, as a practical matter, the agent may be the person with face-to-face contact with the individual.

As discussed above, no opt in will be necessary in many cases because most uses or disclosures will be for the purpose of carrying out "payment" functions and "health care operations," and these two categories encompass a wide range of insurance-related functions. Unless the health insurance carrier elects to seek an opt in or is required to do so under a more restrictive State law, the carrier may use protected health information to carry out such functions without an opt in. Moreover, the business associate rules permit the carrier to disclose such information to the agent without an opt in and, likewise, permit the agent to collect or create protected information on its behalf without an opt in.

#### **4. Opt In Disclosure**

An opt in obtained by an insurance carrier also covers a business associate/insurance agency to the extent that the agency is performing functions on that carrier's behalf.

## **PART II – HIPAA NOTICE CLAUSES**

### **A. Directions for Inserting HIPAA Clauses into Sample GLBA Privacy Notice**

While compliance with HIPAA is not mandated for another two years, we are offering a series of clauses so that agencies that sell health insurance policies can develop one privacy policy that complies with both the GLBA and HIPAA. The proposed clauses in this Part II are sufficient only to the extent that an agency meets two criteria: (1) it is selling health insurance policies directly to individuals; and (2) it shares individuals' health information solely for purposes relating to selling or servicing those policies. To the extent that an agency is selling or servicing group health plans or shares health information for any other purpose, different rules apply.

If these clauses are used, they should be inserted at the end of the GLBA notice on page 22 (following Paragraph 8) but before the signature line. It is important that the signature line follow these HIPAA clauses in order to indicate that individuals have read all of the clauses in the form.

### **B. Text and Clauses to Insert at the End of Sample GLBA Privacy Notice**

THE REMAINDER OF THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW TO OBTAIN ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

### 1. Statement of Our Duties

We are required by the Health Insurance Portability and Accountability Act of 1996 to maintain the privacy of your personal health information and to provide you with this notice of our privacy practices and legal duties. We are required to abide by the terms of this notice. We reserve the right to change the terms of this notice and to make any new provisions effective to all of the personal health information that we maintain about you. If we revise this notice, we will provide you with a revised notice in the following manner [*describe manner in which you will provide a revised notice*].

### 2. Statement of Your Rights

You have a right to know how we may use or disclose your personal health information. This notice informs you of those uses and disclosures. There are certain uses and disclosures of your personal health information that we are permitted or required to make by law without your permission. For all other uses and disclosures, we first must obtain your permission. In addition, you have the following rights:

- (a) The right to request that we place additional restrictions on our uses and disclosures of your personal health information (beyond what the law requires), but we are not obligated to agree to any such additional restrictions.
- (b) The right to access, inspect and copy the protected information pertaining to you that we maintain in our files about you, and the right to have us correct or amend any information that we create in error.
- (c) The right to receive an accounting of the disclosures of your personal health information that we make for purposes *other than* activities related to your treatment, or our payment functions or other health care operations.
- (d) The right to request that you receive communications of personal health information in a confidential manner.
- (e) [*If you provide this notice electronically, you must also include this paragraph:*]

The right to obtain a paper copy of this notice from us on request.

### 3. Permissible Uses and Disclosures of Protected Health Information

- (a) **Payment Functions.** We may use or disclose your health information without your permission to carry out activities relating to reimbursing you for the provision of health care, obtaining premiums, determining coverage, and providing benefits under the policy of insurance that you are purchasing. For example, payment functions may include (but are not limited to) reviewing health care services with respect to medical necessity, coverage under the policy, appropriateness of care, or justification of charges.
- (b) **Health Care Operations.** We also may use or disclose your protected health information without your permission to carry out certain insurance-related activities. These activities include using your protected information for un-

derwriting, premium rating, or other activities relating to the creation, renewal or replacement of another contract of health insurance, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care.

- (c) **Uses Permitted/Required By Law.** We also may use or disclose your protected health information without your written permission for purposes permitted or required by law.
- (d) **Authorized Uses.** All other uses or disclosures of your protected health information will be made only with your written permission, and any permission that you give us may be revoked by you at any time.

#### **4. Complaints About Misuse of Health Information**

You may complain either directly to us or to the Secretary of Health and Human Services if you believe that your rights with respect to our protection of your health information have been violated. To file a complaint with us, you may *[insert statement about how the individual may file a complaint with you, such as "by submitting a complaint in writing that includes as many details (such as names and dates) as possible"]*. You will not be retaliated against in any way for filing a complaint.

#### **5. Contact Person For Filing Complaint or Obtaining Further Information**

*[Insert your organization's contact information, including the name or title and telephone number of the person in your organization that you designate to receive complaints about any misuses of health information or to provide further information about any issue mentioned in the notice. While this a requirement under HIPAA but not the GLBA, it may be easier to designate someone in your organization to respond to complaints or inquiries about any of the topics in your notice – regardless of whether they relate to health or financial privacy.]*

## FLORIDA DEPARTMENT OF INSURANCE INFORMATIONAL BULLETIN 00-004



**BULLETIN 00-004**  
**November 7, 2000**

Florida Department of Insurance  
**Bill Nelson**  
Treasurer, Insurance Commissioner and  
Fire Marshal

**All Insurance Companies Authorized to Write Property and Casualty Insurance, Life and Health Insurance and All Health Maintenance Organizations in the State of Florida**

### **Implementation of the Gramm-Leach-Bliley Act Privacy Provisions**

The Gramm-Leach-Bliley Act, a Federal law enacted on November 12, 1999, requires federal regulators to promulgate regulations by November 13, 2000, to protect the privacy of personal information provided to financial institutions and insurance companies by their consumers. The federal financial regulators responsible for promulgating these regulations have postponed the date for compliance with these rules by entities subject to their jurisdiction until July 1, 2001.

To maintain consistency with the timetable established by federal regulators, the Florida Department of Insurance intends to implement its privacy protections simultaneously with the date established by federal regulators.

The Department anticipates that legislation will be proposed in the 2001 legislative session to address privacy protection.