Compliance with the 1982 NAIC Insurance Information and Privacy Protection Model Act

This memorandum describes agency obligations under the 1982 NAIC Insurance Information and Privacy Protection Act ("1982 Act"). The 1982 NAIC Act is the basis for the insurance-specific privacy regulations already in place in 16 States: Arizona, California, Connecticut, Georgia, Illinois, Kansas (adopted in part), Maine, Massachusetts, Minnesota, Montana, Nevada, New Jersey, North Carolina, Ohio, Oregon, and Virginia.[1] Only agencies doing business in 1982 Act States need to refer to this memorandum.

It is difficult to predict whether the States that have adopted the 1982 Act will replace their current privacy requirements with GLBA-compliant regulations such as those proposed by the NAIC or whether they simply will add GLBA regulations to the 1982 Act requirements already in existence. This difficulty stems from a combination of the varying dynamics of each State's political processes and the GLBA's authorization for the States to impose more protective privacy requirements than the GLBA requires.

Here, we provide an outline of agency obligations under the 1982 NAIC Act that is specifically geared toward explaining how to comply with both the 1982 NAIC Act and the GLBA at the same time. In addition, we have included in Appendix 7 a sample privacy notice form that satisfies *both* the GLBA and the 1982 Act. This form should be used by agencies doing business in 1982 Act States instead of the sample GLBA notice in Appendix 1.

A. The 1982 NAIC Act Protects More Information Than the GLBA

Agencies doing business in 1982 Act States must protect two additional categories of information that are unprotected in certain circumstances under the GLBA.

1. The 1982 NAIC Act protects names and address

The 1982 Act regulates all "personal information," which is individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about character, habits, avocations, finances, occupation, general reputation, credit, health or other personal characteristics. This includes names and addresses.

The GLBA permits disclosure of information such as name and address if the financial institution reasonably believes the information is lawfully made available to the public

1 In addition, Wyoming has adopted its own regulations (not based on the 1982 NAIC Model) governing insurance information.

© Insurance Agent/Broker Coalition, 2001 All Rights Reserved

through other sources. The 1982 Act does not contain this limitation. Accordingly, agencies in a 1982 Act State must treat names and addresses as protected information regardless of whether they believe that information is publicly available.

2. The 1982 NAIC Act protects medical record information

The 1982 Act also protects "medical record information," which is personal information relating to an individual's physical or mental condition, medical history or medical treatment and is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent or legal guardian.

The GLBA does not expressly cover personal health information. The NAIC and NCOIL Model GLBA regulations, however, include provisions protecting health and medical record information. In addition, new regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protect personal health and medical record information.

Although the HIPAA rules likely will preempt both the 1982 Act regulations and the proposed NAIC and NCOIL Model GLBA regulations in most cases, agencies still must be concerned about the requirements for protecting medical record information under the 1982 Act.[2] The primary reason for continued concern about the 1982 Act rules governing medical information is that certain lines of insurance are exempt from coverage under HIPAA but not under the 1982 Act. Benefits excepted under HIPAA include life, disability, and property and casualty insurance, and information gathered in connection with these benefits is not protected. Because the 1982 Act covers life, disability, and property and casualty insurance entities, however, the 1982 Act will continue to apply to these entities' use of medical information even after HIPAA is in place.

B. The 1982 NAIC Act Contains Additional Compliance Obligations

1. More Detailed Privacy Notice Disclosures

Agencies doing business in 1982 Act States must provide a more detailed privacy notice than the notice required by the GLBA. Section C of this memorandum discusses the additional disclosures that must be made by agencies doing business in 1982 Act States. In addition, we have included in Appendix 7 a sample privacy notice form that satisfies both the GLBA and the 1982 Act. This form should be used by agencies doing business in 1982 Act States instead of the sample GLBA notice in Appendix 1.

2 HIPAA does not preempt more restrictive state laws. Like HIPAA, the 1982 Act uses an "opt-in" standard for information sharing, but the 1982 Act contains a broad exception covering information shared for insurance functions that makes it less protective than the HIPAA rules.

© Insurance Agent/Broker Coalition, 2001 All Rights Reserved

2. Opt-In Instead of Opt-Out

The 1982 NAIC Act and GLBA adopt different approaches in terms of an individual's right to prohibit the sharing of personal information. The primary difference is the GLBA's use of an "opt-out" standard and the 1982 Act's use of an "opt-in" standard to govern non-exempted disclosures. The 1982 Act requires agencies to obtain the individual's authorization (a so-called "opt-in") before disclosing any personal or privileged information, including financial and medical information, received in connection with an insurance transaction unless the disclosure falls into an exception.

Information sharing for most insurance-related functions is exempt under both Acts. For these functions, neither an opt-in nor and opt-out is required regardless of whether an agency conducts business in a 1982 Act State. The 1982 Act and GLBA differ, however, with respect to information sharing for marketing purposes. The GLBA contains an exception that the 1982 Act does not include that permits information to be shared to market an agency's own products or any financial products within a joint marketing arrangement. Information sharing is addressed in more detail in Section D, below, where we also describe the requisite elements of a valid authorization. The GLBA joint marketing exception is discussed in more detail in Appendix 4.

3. Imposition of Access Requirements

The 1982 Act includes certain access requirements that do not exist under the GLBA. Specifically, if an individual submits a written request for access to recorded personal information that an agency has about him or her, an agency (or someone acting on its behalf) has 30 business days to do the following:

- Inform the individual of the nature and substance of the recorded personal information;
- Permit the individual to see and copy (in person) the information, or receive a copy of that information by mail. If the information is in coded form, the agency must provide a translation in writing;[3]
- Disclose the identity, if recorded, of the persons or institutions to whom the agency has disclosed that information within 2 years prior to the request. If the identity is not recorded, the agency must provide the names of the persons or institutions to whom such information is normally disclosed; and
- Provide a summary of the procedures for requesting a correction, amendment, or deletion of recorded personal information.

3 If access to medical-record information is requested, the agency may supply that information (as well as the identity of the person or institution that provided it) either directly to the individual or to a medical professional designated by the individual. If the agency elects to provide it to a medical professional, it must notify the individual that it has done so.

© Insurance Agent/Broker Coalition, 2001 All Rights Reserved

The written request for access must reasonably describe the information that is sought and that information must be reasonably locatable and retrievable. Otherwise, the agency is not required to provide access. An agency may charge a reasonable fee to cover the costs incurred in providing copies of information requested.

4. Other Requirements

In addition to the more detailed notice requirements, different information-sharing rules and inclusion of access requirements, the 1982 Act contains several other requirements with which agencies should already be in compliance. For example, the 1982 Act contains requirements for insurance institutions, agents or insurance support organizations that prepare or request investigative consumer reports in connection with an insurance transaction. None of the other 1982 Act requirements intersect with the GLBA and, thus, we do not address them here.

C. The 1982 Act Requires More Details than a GLBA Privacy Notice

1. To Whom and When to Provide the Combined Privacy Notice

The GLBA rules governing to whom and when to provide the initial privacy notice apply to agencies doing business in 1982 Act States. Thus, agencies doing business in 1982 Act States must provide a privacy notice to all customers at the inception of the customer relationship (when an applicant becomes a policyholder), and to all other consumers prior to sharing their information for a non-excepted purpose.

In addition, the 1982 Act requires that notice be provided to individuals in one situation where the GLBA does not. Agencies also must provide their initial privacy notice to an insurance applicant prior to collecting information about him from a source other than the applicant or from public records (for example, from a consumer reporting agency).

As a final matter, agencies doing business in 1982 Act States should be aware that the GLBA contains an annual notice requirement that that 1982 Act does not. In order to be compliant with both Acts, an agency must provide its customers (policy holders) with a copy of its privacy notice at least once every 12 months.

2. Additional Notice Elements Required by the 1982 NAIC Act

The 1982 Act requires that a privacy notice include several elements and details in addition to those required by the GLBA. In order to comply with both the 1982 Act and the GLBA, agencies doing business in States operating under the 1982 NAIC Act will be required to add certain clauses and details to the sample GLBA form in Appendix 1. Sample clauses containing these 1982 Act additions and amplifications are provided in Appendix 7. The

© Insurance Agent/Broker Coalition, 2001 All Rights Reserved

clauses in Appendix 7 can be used to modify the sample GLBA privacy form in Appendix 1 to produce one form that complies with both privacy regimes. In summary, an agency must add clauses that state the following:

- Whether personal information may be collected from persons other than the individuals covered;
- The types of sources and investigative techniques that may be used to collect personal information;
- More detailed information regarding disclosures that fall within exceptions, including the circumstances under which such disclosures may be made without authorization;[4]
- A description of the consumers' rights to access and amend personal information and the manner in which these rights may be exercised
- A statement that the agency collects medical information (if it does in fact collect it);
- A statement that information obtained from a report prepared by an insurance support organization (e.g., a consumer reporting agency) may be retained by that organization and disclosed to other persons.

Instructions for adding these elements to a GLBA notice are provided in Appendix 7.

3. Short-Form GLBA Notices Also Require Additional Information

Under the GLBA, agencies have the option of using a short-form notice for consumers (but not for customers) to whom opt-out forms are presented. The GLBA short form notice rules are more restrictive than the same rules under the 1982 NAIC Act, which permit short form notices to be used for anyone. Agencies must comply with the more restrictive GLBA rules, even in 1982 Act States.

Agencies choosing to use a short form in accordance with the GLBA rules, however, must add certain information to that form if they do business in a 1982 Act State. The requirements for a GLBA short form notice are addressed in the cover memorandum in subsection C.2. The information to be added to a GLBA short form in a 1982 Act State is as follows:

- Personal information may be collected from persons other than the individual or individuals proposed for coverage; and

4 The GLBA only requires detailed information for disclosures that fall within the service provider/joint marketing exception. Otherwise, the notice simply may say that information is shared with third parties "as permitted by law."

© Insurance Agent/Broker Coalition, 2001 All Rights Reserved

- A right of access and correction exists with respect to all personal information collected.

D. Standards for Information Sharing

1. Sharing Information for Insurance-Related Activities

The 1982 Act requires agencies to obtain the individual's authorization before disclosing any personal or privileged information, including financial and medical information, received in connection with an insurance transaction unless the disclosure falls under an exception. Most insurance-related functions are excepted under the 1982 Act and, thus, do not require an opt-in. An individual's information may be disclosed to any insurance institutions, agents insurance support organizations or self-insurer for either the disclosing or receiving institution to perform functions in connection with any insurance transaction involving the individual. Information also may be disclosed to insurance entities to detect or prevent fraud, misrepresentation, or criminal activity in connection with an insurance transaction. Information also may be disclosed to non-insurance institutions who perform business, professional or insurance functions for the disclosing entity (as long as the non-insurance institution agrees not to make further disclosures).

These exceptions are essentially the same as those contained in the GLBA, which means that you can share protected information for insurance purposes without an opt-in or opt-out regardless of whether you are in a 1982 Act State. The rules are the same with respect to health information in a 1982 Act State as long as you are sharing the information for health insurance purposes. Health insurance purposes may include the functions identified above as well as providing information to medical care professionals or medical care institutions for purposes of verifying coverage or benefits, informing the individual of a medical problem of which he may not be aware, or conducting audits to verify the individuals treated by a particular medical professional. Agencies that share health information for *any non-insurance purpose* – such as for marketing purposes – should seek further advice from counsel.

2. Sharing Information for Marketing Purposes

The GLBA and 1982 NAIC Act differ in their treatment of information sharing for marketing purposes. In summary, the 1982 Act exception covering information sharing for marketing purposes is more protective of consumers than the exception for marketing under the GLBA. Agencies must comply with these more restrictive marketing rules in 1982 Act States.

Under the GLBA, no opt-out is required when information is shared: (1) with third parties to market an agency's own products or services; or (2) with third parties to market finan-

© Insurance Agent/Broker Coalition, 2001 All Rights Reserved

cial products offered under a joint marketing agreement between an agency and one or more financial institutions.[5] (See also our discussion of the service provider/joint marketing exception in Appendix 4).

The 1982 NAIC Act's rules for marketing disclosures depend on two things – the kind of information shared and whether the information is shared to market insurance products or other products. For marketing disclosures to anyone for any *non-insurance* products or services, an opt-out standard applies. In other words, although no *opt-in* is required for these disclosures, consumers still must be given an opportunity to *opt-out* of such information sharing. The party receiving the information must agree not to redisclose or reuse the information for any other purpose.

The 1982 Act limits the categories of information that may be disclosed for marketing purposes under this opt-out rule. For certain categories of information an opt-in still is required. No medical information, privileged information (information relating to a claim for insurance benefits) or personal information relating to character, personal habits, mode of living or general reputation can be disclosed to nonaffiliated third parties or to anyone for purposes of marketing non-insurance products without an opt-in.

3. Elements of a Valid Authorization

Unlike the GLBA, the 1982 NAIC Act requires substantive disclosures in two documents – the privacy notice and the authorization form. (In contrast, under the GLBA, all substantive disclosures are made in the privacy notice – the opt-out form simply states the methods by which the opt-out right may be exercised.) The disclosures required to be made in an authorization form are in addition to those required in the notice. Agencies do not need to make these additional disclosures, however, unless they actually are seeking an authorization. These disclosures should not be combined with the initial privacy notice but, instead, be made separately on the authorization form.

When an authorization is required in a 1982 Act State, the authorization form must be written in plain language, signed by the individual and dated. In addition, the authorization form must:

- Specify the types or categories of persons authorized to disclose information about the individual;
- Specify the nature of the information authorized to be disclosed;
- Names the insurance institution or agent requesting the authorization and

5 Even though no opt-out is required, notice must be provided and a contract must be in place between the agency and the third party that prohibits the third party from any further sharing of the information.

© Insurance Agent/Broker Coalition, 2001 All Rights Reserved

identify by generic reference the representatives of the insurance institution to whom the individual is authorizing the information to be disclosed;

- Specify the purposes for which the information is collected;
- Advise the individual or a person authorized to act on his behalf that the individual or representative is entitled to a copy of the authorization form.
- Specify the length of time that the authorization will remain valid, which can be no longer than:
    - If the authorization is signed for the purpose of collecting information in connection with an application for an insurance policy, policy reinstatement, or request for a change in policy benefits:
        - 30 months from the date of the authorization, if the application or request involves life, health or disability insurance;
        - 1 year from the date of the authorization, if the application or request involves property or casualty insurance;
    - In the case of authorizations signed for the purpose of collection information in connection with a claim for benefits:
        - The term of coverage of the policy if the claim is for a health insurance benefit;
        - The duration of the claim if the claim is not for a health insurance benefit.

© Insurance Agent/Broker Coalition, 2001 All Rights Reserved