

Third National HIPAA Summit

Gramm-Leach-Bliley
State Law Implementation



October 26, 2001

Robert W. Woody

LeBoeuf, Lamb, Greene & MacRae, I.I.P.
a limited liability partnership including professional corporations

Gramm-Leach-Bliley



Gramm-Leach-Bliley Act signed into law on November 12, 1999



Main objective was to eliminate Depression-era barriers to affiliations among, banks, securities, and insurance firms.



Also included privacy provisions applicable to all "financial institutions"

Gramm-Leach Bliley Act

- ⌚ **Scope of Privacy Provisions (Title V)**
GLB applies to a financial institution's disclosure of its consumers' nonpublic personal information to nonaffiliated third parties. GLB does not apply to the sharing of information between affiliates.



Preemption

- ⊗ **GLB preempts state privacy laws that are deemed to be inconsistent with GLB's privacy provisions.**
 - ☞ **A state law that affords greater privacy protection is not deemed to be inconsistent with GLB.**
 - ☞ **As of now, no state has passed GLB-related privacy laws that apply to financial institutions other than those regulated by departments of insurance.**





GLB preserved "functional regulation" meaning that those entities that regulated banks, securities, and insurance firms before GLB was enacted will continue to do so under GLB.

- ⊗ Securities firms = SEC
- ⊗ Banks = State or federal banking regulators
- ⊗ Insurance = State insurance regulators

Regulations

GLB directs regulators of the financial institutions to issue regulations addressing the privacy provisions.

-  **Final regulations for financial institutions regulated by federal agencies (including the Office of the Comptroller of the Currency, Federal Trade Commission, and the Office of Thrift Supervision) were issued on or about May 2000**
-  **State insurance regulators are to issue regulations applicable to insurers**



Can Congress tell state insurance regulators how to regulate privacy?



Probably unconstitutional



It doesn't matter. State insurance regulators will implement GLB privacy provisions anyway.



Substantive Provisions of GLB

Notice

GLB requires that information relating to a financial institution's privacy practices must be disclosed to its consumers on an initial and annual basis.

Opt Out

A consumer must be given the opportunity to “opt out” of the disclosure of their information to nonaffiliated third parties. GLB provides a number of exceptions to this general rule.

Joint Marketing / Servicing Exception

-  **To perform services for the financial institution or functions on the financial institutions behalf.**
-  **Joint marketing agreement between the two financial institutions.**



State Actions

 **How have states responded?**

 **Heavily influenced by National Association of Insurance Commissions (NAIC)**

 **Three Groups**


 **1982 NAIC Model Act**



 **1999 NAIC Model Regulation**

 **Other**



States without existing privacy laws before enactment of GLB

 **75% (26 out of 34) of these states have passed substantive privacy statutes or regulations (AL, AR, CO, DE, DC, FL, HI, ID, IN, IA, KY, LA, MI, MS, MO, NE, NH, NM, NY, SC, SD, TN, TX, WV, WI, WY)**

-  **Most new privacy laws are similar to the NAIC Model Regulation.**
-  **There are some variances within the individual states.**



State Implementation

- ⊗ **The privacy provisions of this model act were not widely implemented as only 17 states enacted laws with provisions that were based on or related to it (AZ, CA, CT, GA, IL, KS, ME, MA, MN, MT, NV, NJ, NC, OH, OR, VA, WY).**
- ⊗ **Still in place in all except IL, KS, VA**

1982 NAIC Model Act




Notice Requirements

Long Form


 **Requires disclosures about information collected, information practices, parties receiving information, access to information and ability to correct information.**


Short Form

 **Consisting of four short disclosures, this form may be substituted in place of the long form as long as the person receiving the notice can obtain the long form upon request (NAIC Model, § 4 (C)).**



Parties Receiving Notice

 **Either the long form or short form is to be given to all applicants or policyholders in connection with an insurance transaction (NAIC Model, § 4 (A)).**

 **Certificate holders insured under a group policy are considered to be applicants or policyholders if the group coverage is “individually underwritten”**



Delivery of the Notice



Initial Notice

Application: the notice must be supplied upon delivery of the policy or certificate or at the time personal information is collected from a source other than the applicant.



Policy Renewal

Must be provided to the policyholder no later than the renewal date (but must be provided at least once every two years).



Opt In Required for Disclosures

- ⊗ **Except for certain specific disclosures, the express written consent of the individual is needed for disclosure of information about that individual collected or received in connection with an insurance transaction**
- ⊗ **Some types of information may be disclosed by an insurer solely in connection with the marketing of a product or service if the individual has been given an opportunity to opt out**

1999 NAIC Model Regulation



This model regulation was created with the goal of consistent privacy provisions amongst the states.



Federally regulated financial institutions are subject to one set of regulations, but state privacy regulation means insurers will be subject to numerous different regulations.



Gramm-Leach-Bliley was designed to streamline the financial services industry, so a patchwork of regulations could put insurers at a competitive disadvantage.

Substantive Provisions

Information Subject to Regulations

-  **Nonpublic personal health information**
-  **Nonpublic personal financial information**



Group Certificateholders

Notice not required to individuals under group coverage if:

-  **a notice is provided to the group policyholder**
-  **no information is shared outside of exceptions**

Consumer/Customer

The NAIC Model Regulation, consistent with the regulations of the federal regulators, differentiates between a consumer and a customer.

-  **A consumer is an individual who seeks to obtain, obtains, or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes.**
-  **A customer is a consumer with a continuing relationship with a licensee.**









Delivery

The Privacy Notice must be provided to customers initially no later than establishment of the customer relationship and annually thereafter.



Financial Information Exceptions






Privacy Policy notices and opt outs not required for disclosures related to:

-  **Joint Marketers or Service Providers
(exception from opt out only)**
-  **Underwriting insurance**
-  **Reinsurance transactions**
-  **Account administration**
-  **Investigating fraud**
-  **Processing premium payments**
-  **Processing claims**
-  **In connection with sales or mergers**



Additional impact on Life and Health Insurers








Opt In (Health Information)

-  **Consumers or customers must give affirmative consent (*i.e.*, opt in) before health information can be disclosed**
-  **Consent is revocable at any time**
-  **Can be in writing or, if customer agrees, electronic form**
-  **Applies to all lines but primary impact is on life and health**
-  **Will result in additional costs to produce and process opt ins**



Health Opt In Exceptions

 **Worded differently from financial information exceptions, but similar in some respect. Include:**

-  **Underwriting**
-  **Claims administration, adjustment and management**
-  **Reinsurance**
-  **Ratemaking functions**
-  **Loss control**
-  **Risk management**
-  **Utilization review**



Examples of state deviation from model

- ⊗ **Individual certificateholders under group coverages must receive notice (*e.g.*, Hawaii)**
- ⊗ **Insurers have choice of sending GLB privacy notice or more specific notice required by the 1981 Model Act (*e.g.*, Arizona)**

Problem States



Minnesota

- ⊗ **Must comply with the stricter of the Model Act or the Model Regulation on an item-by-item basis**
- ⊗ **Opt in required to share for marketing purposes**
- ⊗ **Applicants must get privacy notices**



Montana

- ⊗ **Applicants must get privacy notices**
- ⊗ **Certain individual group certificateholders must get notices**
- ⊗ **Opt in required**
- ⊗ **Business exceptions available only with agreement from third party that it will not further disclose information**

Future Privacy Regulation?



California SB 773 was nearly adopted this year, but ultimately failed

⊗ **Opt out for affiliate sharing**

⊗ **A much more limited exception for joint marketing**

⊗ **Substantial penalties**

☞ **Negligent Disclosure = \$2,500/per violation**

☞ **Willful or Subsequent Disclosure = \$250,000**

Other GLB State Issues



GLB is a federal law but it prohibits states from doing certain things and requires states to do other things.




If banks can now sell insurance, where is the line between federal banking and state insurance regulatory authority over a bank?



Answer: Insurance regulators can go about their business, but there are certain things they cannot do:

- ⊗ "Prevent or restrict" affiliations between banks and insurers
- ⊗ Discriminate against insurance entities that are affiliated with banks
 - ☞ Rules for insurers affiliated with banks generally must be the same as for insurers not affiliated with banks
 - ☞ If they are not the same, they must not discriminate against insurers affiliated with banks

- ③ Regulate insurance sales, solicitation, or cross-marketing activities of insurers affiliated with banks, except for 13 safe harbors. For example states can say:
 - ☞ No "bundling." Banks cannot tell customers "you don't get a mortgage unless you buy your homeowners insurance from us"
 - ☞ No sharing of health information without consent (except in connection with bank's activities as insurance agent or broker)
 - ☞ No sharing of customer confidential information to any entity not affiliated with the bank without the customer's express consent

 There will inevitably be disputes between federal and state regulators over where authority ends and the other's begins.

 Expedited judicial review of such disputes by the appropriate U.S. Court of Appeals.





 Judgment must be rendered within 60 days

 Must be decided "without unequal deference" to either federal or state law.



National Association of Registered Agents and Brokers (NARAB)

- ⊗ Private, non-profit entity
- ⊗ Will be created only if a majority of states fail to enact uniform or reciprocal agent and broker licensing laws by November, 2002.
- ⊗ Once its created, any agent or broker can join and will operate only under authority granted by NARAB. Most state laws preempted.

-  There are questions about what constitutes an acceptable level of "uniformity" or "reciprocity"
-  Most agree that a sufficient number of states have acted to prevent the creation of NARAB.
-  A number of big states like California, Texas, and New York have not
-  Question: How much uniformity has really been achieved? Will Congress take a second look?

Third National HIPAA Summit

QUESTIONS?



LeBoeuf, Lamb, Greene & MacRae, I.I.p.
a limited liability partnership including professional corporations

LeBoeuf,
Lamb,
Greene &
MacRae, I.L.P.

a limited liability partnership including professional corporations