

Benefit Brief



SUBJECT: Gramm-Leach Bliley Act Compliance Requirements for Insurance Producers in Pennsylvania

DATE: January 19, 2006

This Benefit Brief summarizes the requirements for group health insurance producers in Pennsylvania with respect to the Gramm-Leach-Bliley Act and the corresponding state regulations. Insurance producers in Pennsylvania who are selling individual products may have different compliance obligations under these laws.

The Gramm-Leach-Bliley Act (the "GLBA"), which became effective on July 1, 2001, requires that insurance brokers protect and disclose their policies and practices for protecting the privacy of the non-public personal information, including both financial information and health information. The GLBA requirements are similar to the requirements of the HIPAA privacy and security rules. The state regulations provide that producers who have complied with the HIPAA privacy will have fulfilled their obligations to comply with the GLBA as stated in Pennsylvania Regulations.

Failure to comply with the GLBA regulations is considered an unfair insurance practice, which could result in fines, lawsuits and/or revocation or suspension of a producer's license.

Requirements and Compliance Dates under the Pennsylvania Regulations

| Rule | Compliance Required by: | Summary of Requirements |
|---|--------------------------------|---|
| Privacy of Financial Information | July 1, 2001 | Requires producers to send a Privacy Notice to employer clients (in some situations) |
| Privacy of Health Information | October 26, 2002 | All requirements contained in the HIPAA privacy rule, including the requirement that authorization is obtained before disclosure of health information for any reason other than fulfillment of an insurance function (as described below). |
| Safeguarding of Health Information (Security) | March 1, 2005 | Producer must adopt a written "Information Security Program" or Security Policy. |

Privacy Notice

An independent insurance producer is required to send a privacy notice to its group insurance clients EXCEPT FOR THOSE CLIENTS:

- Whose health coverage is provided through insurance companies; and
- Who receive a Privacy Notice from those insurance companies.

If the producer discloses any non-public personal financial information about the employees of the client to anyone other than the insurance company, then the producer would need to send that client a Privacy Notice.

Therefore, Privacy Notice, in most cases, will only need to be sent to your **self-funded** clients. A copy of a sample Privacy Notice is attached for your review. Your Privacy Notice should be sent once per year to your clients and can either be hand delivered or sent by U.S. mail. They can be sent electronically only if the client has agreed to receive the notice electronically.

If you determine that you disclose personal financial information to a non-affiliated third party for reasons other than performing insurance functions (as described below), then you also have to include an "opt-out" provision in your notice. The "opt-out" allows the group to request that you do not disclose the financial information of its employees.

Non-Public Personal Financial Information

Includes:

- Personally identifiable financial information (such as any information obtained by the Producer in connection with providing an insurance product to the individuals' employer or information that connects the individual to a specific carrier); and
- Any list, description or other grouping of individual that is derived from personally identifiable financial information that is not publicly available.

These lists include lists of individuals' names and street addresses that includes information that is not publicly available such as account numbers or birthdates. If the list includes information about the insurance carrier, the list would be considered Non-Public Personal Financial Information.

Insurance Functions

Include:

- Claims administration
- Claims adjustment (investigation, negotiation, settlement)
- Detection, prevention, investigation or reporting of actual or potential fraud
- Underwriting
- Policy placement or issuance
- Loss control
- Ratemaking
- Reinsurance and excess loss insurance
- Risk management
- Case management
- Disease management and wellness
- Utilization review
- Grievance and complaint procedures
- Internal administration of compliance, managerial and information systems
- Auditing
- Replacement of a group health plan
- Disclosure that is required by law or to comply with legal process
- Any other disclosure permitted under the HIPAA privacy rules

Information Security Program

The Pennsylvania regulations require that every Producer implement a comprehensive information security program that addresses administrative, technical and physical safeguards for personally identifiable financial and health information maintained electronically. The regulations discuss safeguarding the confidentiality of the information, protecting against reasonably anticipated

threats and preventing unauthorized use of the information that could result in substantial harm or inconvenience to the customer.

Examples of how a Producer could comply with these requirements include:

- Conducting a **risk assessment** to assess threats and sufficiency of policies, procedures and safeguards that are already in place.
- Designing a **security policy and program** to control identified risks, including training staff and regularly testing the controls, systems and procedures of the program.
- Overseeing **service provider arrangements**
- **Monitoring and modifying the program** in light of changes in technology, sensitivity of information maintained, internal or external threats, etc.

These examples are not requirements, but are methods of demonstrating compliance with the law. Each producer needs to determine the best method and appropriate steps based on the types and amounts of health and financial information that it maintains, as well as the risk to the security of the information. Compliance with the HIPAA security rules (with the addition of steps to protect financial information) would meet or exceed your obligations under the GLBA.

If you have any questions about how to implement the requirements of the GLBA, please contact Judy Griffith at The Benecon Group at jgriffith@benecon.com, or the number shown below.

This Benefit Brief is provided for informational purposes only and does not constitute legal advice. The Benefit Brief contains only a summary of the applicable legal provisions and does not purport to cover every aspect of any particular law, regulation or requirement. Depending on the specific facts of any situation, there may be additional or different requirements. Please use this Benefit Brief as a guide and not as a definitive description of your compliance obligations.

SAMPLE GLBA PRIVACY NOTICE (IF OPT-OUT IS NOT REQUIRED)

To:

From:

Subject: Annual Privacy Notice

Date:

Broker Name has always been committed to providing its customers with outstanding products and services and to respecting the privacy rights of its customers. This Privacy Notice is provided to you as required by state and federal law. We will be sending you this Notice every twelve months for as long as you are a customer of **Broker Name** or whenever we change our privacy practices.

Information we collect and the ways that we collect it

Broker Name collects nonpublic personal financial information and nonpublic personal health information about your employees from the following sources:

- Information we receive from you and your employees on applications and on other written communications;
- Information about your transactions with us, our affiliates or other nonaffiliated third parties; and
- Information we receive from reinsurance companies.

Examples of this information include social security number, date of birth, marital status, claims amounts, major illness, other insurance information and employment information.

We collect this information using the following means of communication: written, in-person, telephone, facsimile, electronically and online.

How we share employee information

We don't share information about our customers' or former customers' employees with affiliated or non-affiliated third parties other than as required or permitted by law. For example, we may share all of the information described above with non-affiliated third parties for the following reasons:

- Underwriting, shopping the renewal, rating, placement and providing quotes for insurance
- Resolving claims and other disputes
- Responding to client inquiries
- To individuals or entities who are assessing our legal compliance

We restrict access to the nonpublic personal financial information and health information about your employees to those individuals within our company who need to know that information to provide services to you. These individuals are trained and required to maintain our privacy policies and procedures. We maintain physical, electronic and procedural safeguards that comply with federal and state regulations to protect the personal information of your employees. Individuals who violate these policies and safeguards are subject to disciplinary action.

If you have any questions about how we protect the privacy of your employees or for a copy of our privacy policy, please give us a call. Thank you for placing your confidence in the Benecon Group.