Gramm-Leach-Bliley
What Do Insurance Agents Need to Know About it?

By Bridgette O’Connor,
PHI365 Manager, GRA Benefits Group

HIPAA, Affordable Care Act and now Gramm-Leach-Bliley. You are probably thinking, another one? It’s disconcerting how many laws there are that affect how you handle client information. In this article, I will provide a description of this law and some compliance solutions.

These laws all have the same goal: to protect personal information. They all require similar obligations to protect that information. Therefore, if you are compliant with at least one law, you are almost in compliance with all three. Let’s take a closer look at GLB.

Enacted in 1999, GLB allowed for drastic changes in the financial service industry. The law’s main feature permitted financial institutions, such as investment banks and insurance companies, to consolidate. Nearly 15 years later, the focus of the law has shifted to the Privacy and Safeguards rules.

GLB has two definitions that are important to know: (1) Financial institutions are businesses that engage in financial activities, such as banking, securities or insurance. (2) Financial activities are insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death. Acting as an agent or broker for insurance is also considered a financial activity.

Where HIPAA only applies to health agents, GLB applies to all types of insurance agencies and agents as described in the above definitions.

GLB is designed to protect your client’s personal financial information, or as the law defines it: nonpublic personal information (NPPI). This NPPI is any information that a client may share to obtain insurance pricing or a policy. It also includes any information you may gather about that client during a transaction that isn’t publically available, such as through government records, telephone books or newspapers.

The Privacy and Safeguards rules of Gramm-Leach-Bliley have three overarching elements:

1. Provide a privacy notice.
2. Provide an opt-out form.
3. Institute data security and integrity mechanics to protect NPPI.

The first two elements go hand-in-hand and are generally used at the same time. The industry standard is to send these two documents when you first establish a new relationship with a client. Then reissue the notice and opt-out form annually. The notice describes your privacy policies: what information you collect, how you collect and store it and to whom you disclose that information. The opt-out form then allows the clients to opt-out of certain disclosures to unaffiliated parties that you list in the notice.

For group insurance policies, providing the notice to the plan sponsors satisfies the notification obligations. Each individual plan or policy requires its own privacy notice. If it is a health insurance policy, you must include HIPAA statements. And if it is an individual health plan from the Federal Marketplace, you should also include privacy statements required by your agent agreement.

The Federal Trade Commission (FTC) offers guides to writing your own GLB privacy notice.

The third obligation is deemed the Safeguards Rule. This is similar to HIPAA’s Security Rule. The Safeguards Rule requires financial institutions to protect NPPI using administrative, technical and physical safeguards. To do so you should have an information security plan that describes how the
company will protect the confidentiality and integrity of clients’ NPPI. The plan should also:

- Designate at least one employee to coordinate the information security program.
- Include a documented risk analysis.
- List effective safeguards used for controlling risks.
- Schedule tests and reviews for program and future risk analyses.
- Provide policies for selecting service providers and overseeing their handling of NPPI.

For insurance companies and agencies, GLB is enforced under state insurance law, i.e., by state insurance authorities and attorneys general. Note that if you have an information breach, such as losing an unencrypted laptop, you may be susceptible to as many as three different fines, depending on the type of information breached, i.e. GLB, HIPAA and PPACA.

The FTC has been more active in enforcing Gramm-Leach-Bliley recently. Under a section of the FTC Act the FTC has the authority to examine privacy policies and practices for deception and unfairness. They are issuing fines that compete with some of HIPAA’s largest fines – in the millions of dollars.

If all this compliance talk seems too overwhelming, consider hiring a consultant to assist in implementing all the necessary rules and regulations. GRA Benefits Group offers a compliance program geared specifically toward insurance agents.

Remember, nothing will help build trust between agents and their clients more than showing care and sensitivity around personal information. And there is no better way to accomplish that than knowing the legal requirements and how to meet them.

As the PHI365 manager at GRA Benefits Group, Bridgette O’Connor consults with agents on moving toward HIPAA and Gramm-Leach-Bliley compliance.

“As my retail agency experience helps me understand what our agents and CSRs are faced with on a daily basis. I’m able to speak from first-hand experience and assist agents with submissions and market considerations.”

Erin Dey
Director of Sales and Agency Relations