

GLBA Compliance Guide for Insurance Companies

Date: 03/01/2025

Author: Gerria LeSure

1. Overview of GLBA (Gramm-Leach-Bliley Act)

The **Gramm-Leach-Bliley Act (GLBA)** is a **U.S. federal law** that requires **financial institutions**, including **insurance companies**, to **protect consumer financial data**.

Key Compliance Areas:

- ✓ **Safeguards Rule** – Requires data security measures.
 - ✓ **Privacy Rule** – Governs collection & sharing of customer data.
 - ✓ **Pretexting Rule** – Prevents unauthorized access to private information.
-

2. Who Must Comply?

GLBA applies to any business that:




- **Provides financial services**, including **insurance** (auto, health, life, business, home).
- **Collects or stores consumer financial information** (claims data, credit reports, underwriting records).

For insurance companies, this means:

- ✓ You must **disclose** how customer data is collected, stored, and shared.
 - ✓ You must **protect** customer financial data from breaches or unauthorized access.
 - ✓ You must have an **incident response plan** in case of a **data breach**.
-

3. GLBA & Data Protection in the Insurance Industry

Insurance companies handle **sensitive consumer data**, including:

-  **Personally Identifiable Information (PII)** – Name, SSN, Address, DOB
-  **Financial Data** – Credit scores, banking details
-  **Claims Information** – Medical records, accident history

Failure to comply with GLBA can result in:

- ✗ **Fines up to \$100,000 per violation** for institutions.
- ✗ **Personal liability fines up to \$10,000 per executive**.
- ✗ **Consumer lawsuits** for data breaches.

4. How Insurance Companies Can Ensure GLBA Compliance

- ✔ **Implement a Data Security Program** – Encrypt financial & customer data.
 - ✔ **Limit Employee Access to Sensitive Information** – Use **Role-Based Access Control (RBAC)**.
 - ✔ **Provide Customers with Privacy Notices** – Explain how their data is used.
 - ✔ **Develop an Incident Response Plan** – Have a process for responding to data breaches.
 - ✔ **Audit Third-Party Vendors** – Ensure service providers follow GLBA compliance rules.
-

5. Summary Table – GLBA Compliance Checklist

GLBA Requirement	Action for Insurance Companies
Develop a Data Security Program	Encrypt customer financial data
Provide Privacy Notices	Disclose how customer data is collected & used
Implement Access Controls	Use RBAC & MFA to limit access to sensitive PII
Monitor & Audit Vendors	Ensure third-party compliance with GLBA
Create an Incident Response Plan	Have a breach response strategy