Privacy & Data Protection Risk Assessment – Insurance Industry

Date: 03/01/2025
Assessed by: Gerria LeSure

1. Executive Summary

Overview

This assessment evaluates **privacy and data protection risks** for a **large insurance company** (simulated as State Farm), using **GLBA, CCPA, and NIST Privacy Framework** compliance principles.

Key Findings

- 🚨 **Data Privacy Gaps** – No clear **opt-out process** for data sharing (CCPA risk).
- 🔓 **Access Control Risks** – Employees have **excessive access** to customer PII.
- 🏢 **Third-Party Vendor Weaknesses** – No **regular security audits** for vendors handling sensitive insurance data.
- 🔐 **Encryption Concerns** – Some legacy systems **store unencrypted PII**, increasing data breach risks.
- ⚠️ **No Incident Response Plan (IRP) for Data Breaches** – High risk of **regulatory penalties** for slow breach response.

Recommended Actions

✓ **Implement customer opt-out mechanisms** for data sharing (CCPA compliance).
✓ **Enforce Role-Based Access Control (RBAC)** to limit PII exposure.
✓ **Mandate third-party vendor security audits** and compliance monitoring.
✓ **Encrypt all customer PII** in storage and transit.
✓ **Develop and test a Data Breach Response Plan** following NIST 800-61 guidelines.

---

2. Business Context & Compliance Overview

Company Profile (Simulated – State Farm Insurance)

📌 **Industry:** Insurance (Auto, Home, Life, Business)
📌 **Size:** Large (50,000+ employees, multiple locations)
📌 **Data Processed:**

- **Personally Identifiable Information (PII):** Name, DOB, SSN, Address
- **Financial Data:** Credit history, claims, payments
- **Medical & Claims Records:** Accident reports, healthcare data
- **Customer Communication Logs:** Calls, emails, online support

Relevant Privacy & Data Protection Regulations

Regulation	Requirement	Applicability to Insurance
GLBA (Gramm-Leach-Bliley Act)	Requires financial institutions to protect customer PII	Insurance companies must implement strict data security policies
CCPA (California Consumer Privacy Act)	Gives consumers rights to access, delete, and opt out of data sharing	Insurance companies handling CA residents' data must comply
NIST Privacy Framework	Provides best practices for privacy risk management	Helps establish data protection and governance policies

---

3. Privacy & Security Risk Assessment Findings

The following table highlights key **privacy & data protection risks**, their **impact levels**, and **recommended mitigations**.

Privacy Risk Category	Security Gaps Identified	Risk Level	Recommendations
Customer Data Privacy (GLBA, CCPA)	No clear opt-out process for data sharing	**High**	Implement an **automated opt-out system**
Third-Party Risk Management	Vendors handling PII are not regularly audited	**High**	Conduct **annual security audits** for vendors
Data Retention & Deletion	No automated deletion of expired customer records	**High**	Enforce **data retention policies** with auto-deletion
Encryption & Data Storage	Some legacy systems store PII unencrypted	**Critical**	Implement **full-disk encryption & tokenization**
Access Control & Internal Permissions	Employees have excessive access to PII	**High**	Apply **Role-Based Access Control (RBAC)**
Incident Response & Breach Notification	No structured data breach response plan	**Critical**	Develop a **Data Breach Response Plan**

---

4. Risk Matrix & Data Protection Recommendations

Privacy Risk Matrix

The **risk matrix** categorizes threats based on **likelihood and impact**, helping prioritize risk mitigation efforts.

Risk	Likelihood (1-5)	Impact (1-5)	Overall Risk (L x I)	Mitigation
No customer opt-out mechanism	4	3	12 (Moderate)	Implement **CCPA-compliant opt-out system**
No security audits for vendors	5	4	20 (High)	Require **annual security audits**
No encryption on legacy data	5	5	25 (Critical)	Enforce **data encryption (AES-256)**
Employees have excessive PII access	5	4	20 (High)	Implement **Role-Based Access Control (RBAC)**
No Incident Response Plan	5	5	25 (Critical)	Develop **Data Breach Response Playbook**

---

5. Recommended Remediation Plan

✅ **Short-Term Fixes (0-3 Months)**

1. **Develop a Consumer Privacy Policy** – Publish a policy explaining data rights and CCPA compliance.
2. **Restrict Employee Access to PII** – Enforce **Role-Based Access Control (RBAC)**.
3. **Implement Opt-Out Mechanisms** – Allow customers to control data sharing preferences.

🚀 **Mid-Term Fixes (3-6 Months)**

1. **Encrypt Sensitive Data** – Implement **AES-256 encryption** for data at rest.
2. **Conduct Security Awareness Training** – Train employees on **data protection best practices**.
3. **Begin Third-Party Security Audits** – Assess vendors handling PII for compliance risks.

🔒 **Long-Term Fixes (6-12 Months)**

1. **Develop a Data Breach Response Plan (IRP)** – Prepare for data leaks & cyber incidents.
2. **Establish Continuous Compliance Monitoring** – Implement tools to track **privacy compliance**.
3. **Deploy SIEM & Threat Detection** – Monitor real-time threats to **sensitive customer data**.

---

6. Conclusion & Next Steps

This assessment identified key **data protection weaknesses** in **customer privacy, access control, encryption, and vendor risk management**. To improve **compliance and security**, the insurance company must:

1. **Implement better privacy controls (CCPA & GLBA compliance).**
2. **Reduce unauthorized employee access to customer data.**
3. **Strengthen vendor security audits and data protection policies.**
4. **Develop an Incident Response Plan (IRP) for privacy breaches.**
5. **Encrypt all sensitive customer data using AES-256.**

📌 **Next Steps:**
✅ Implement **privacy policies & opt-out mechanisms**
✅ Develop **data encryption & access control policies**
✅ Test **incident response drills for data breaches**