ChecklistGuro

Insurance Data Security Compliance Checklist

Data Governance & Policies

Review and adherence to established data governance frameworks and security policies.

Data Governance Framework Adopted?

□ COBIT

□ DAMA-DMBOK

□ Other (Specify)

Summary of Data Governance Policy

Write something...

Number of Data Stewards

Enter a number...

Last Policy Review Date

Enter date...

Policy Access Method

□ Centralized Repository

□ Shared Drive

□ Intranet

Describe Data Classification Scheme

Write something...

Access Controls & Authentication

Verification of role-based access controls, multi-factor authentication, and privileged access management.

Multi-Factor Authentication (MFA) Enabled?

□ Yes

□ No

□ Partial (some systems)

Password Complexity Requirements?

□ Strong (min length, special chars, rotation)

□ Moderate

□ Weak/None

Maximum Login Attempts Before Lockout

Enter a number...

Role-Based Access Controls (RBAC) Implemented?

□ Yes

□ No

□ Partial

Last Review of Access Control Lists (ACLs)

Enter date...

Which user roles have access to sensitive data?

□ Underwriter

□ Claims Adjuster

□ Actuary

□ Customer Service

□ IT Support

Data Encryption & Storage

Assessment of data encryption methods (at rest and in transit) and secure storage practices.

Encryption Method (Data at Rest)

□ AES-256

□ RSA

□ Triple DES

□ Other - Specify in Long Text

Encryption Method (Data in Transit)

□ TLS 1.3
□ TLS 1.2
□ SSL 3.0 (Not Recommended)
□ Other - Specify in Long Text

Key Rotation Frequency (Days)

Enter a number...

Detailed Description of Encryption Key Management Process

Write something...

Storage Type (Sensitive Data)

□ Cloud Storage (Specify Provider)
□ On-Premise Storage
□ Hybrid Storage

Storage Security Assessment Report (Optional)

Upload File

Data Loss Prevention (DLP)

Evaluation of DLP measures to prevent unauthorized data leakage.

Number of DLP Rule Violations in Last 30 Days

Enter a number...

DLP Software Version in Use

- □ Version 1.0
- □ Version 2.0
- □ Version 2.1
- □ Latest Version

Data Types Protected by DLP Rules (Select all that apply)

- □ Personally Identifiable Information (PII)
- □ Financial Data
- □ Health Information (PHI)
- □ Proprietary Information

Summary of Recent DLP Incidents and Remediation Steps

Write something...

DLP Rule Monitoring Frequency

- □ Real-time
- □ Hourly
- □ Daily

Upload Configuration File for DLP System

Upload File

Incident Response & Recovery

Examination of incident response plans, data backup procedures, and disaster recovery capabilities.

Date of Incident Detection

Enter date...

Time of Incident Detection

Detailed Description of the Incident

Write something...

Incident Severity Level

- ☐ Low
- ☐ Medium
- ☐ High
- ☐ Critical

Systems Affected

□ Claims System
□ Policy Administration System
□ Customer Database
□ Internal Network
□ External Website

Containment Actions Taken

Write something...

Estimated Number of Records Potentially Affected

Enter a number...

Date of Incident Containment

Enter date...

Lessons Learned and Recommendations

Write something...

Third-Party Risk Management

Review of security assessments and contractual obligations for vendors handling insurance data.

Vendor Security Assessment Completed?

□ Yes

□ No

□ In Progress

Vendor Risk Score (1-100)

Enter a number...

Last Security Assessment Date

Enter date...

Vendor Security Assessment Report

Upload File

Contractual Security Requirements Defined?

□ Yes

□ No

□ N/A

Summary of Vendor's Security Practices

Write something...

Security Domains Covered in Assessment

□ Physical Security
□ Network Security
□ Data Encryption
□ Access Controls
□ Application Security

Compliance & Regulatory Requirements

Verification of adherence to relevant regulations (e.g., GDPR, CCPA, state-specific laws).

Applicable Regulations (Select all that apply)

□ GDPR
□ CCPA
□ HIPAA
□ State-Specific Privacy Laws (Specify in LONG_TEXT)
□ NAIC Model Laws

Specific State Privacy Laws Applied (If selected above)

Write something...

Last Regulatory Compliance Training Date

Enter date...

Frequency of Regulatory Compliance Reviews (per year)

Enter a number...

Recent Regulatory Audit Status

□ Pass

□ Conditional Pass

□ Fail

Uploaded Documentation (e.g., Audit Reports, Compliance Certificates)

Upload File

Employee Training & Awareness

Confirmation of employee training programs on data security best practices and incident reporting.

Last Data Security Training Completion Date

□ Within Last 3 Months

□ 3-6 Months Ago

□ 6-12 Months Ago

□ Over 12 Months Ago

Topics Covered in Data Security Training

□ Phishing Awareness

□ Password Security

□ Data Handling Procedures

□ Incident Reporting

□ Secure Remote Access

Employee Name

Write something...

Next Scheduled Data Security Refresher Date

Enter date...

Summary of Data Security Best Practices (Employee Confirmation)

Write something...

Vulnerability Management & Patching

Assessment of vulnerability scanning and patch management processes for systems handling insurance data.

Last Vulnerability Scan Frequency (Days)

Enter a number...

Vulnerability Scanning Tool Used

□ Nessus
□ Qualys
□ Rapid7
□ Other

Scanning Scope (Check all that apply)

□ Production Servers
□ Development Servers
□ Databases
□ Network Devices

Last Remediation Effort Completion Date

Enter date...

Percentage of Critical Vulnerabilities Remediated within SLA

Enter a number...

Patch Deployment Methodology

- □ Manual
- □ Automated
- □ Hybrid

Data Minimization & Retention

Review of practices to minimize data collection and securely manage data retention periods.

Maximum Data Retention Period (Years)

Enter a number...

Data Destruction Method

- □ Secure Erasure
- □ Physical Destruction (e.g., Shredding)
- □ Decommissioning with Data Wipe

Last Data Retention Policy Review Date

Enter date...

Data Types Subject to Retention Limits

□ Customer PII

□ Claims Data

□ Policy Documents

□ Financial Records

□ Marketing Data

Justification for Data Retention Periods (if exceeding regulatory limits)

Write something...