autorabit

EBOOK

Everything You Need to Know about Compliance and the Insurance

Remaining Compliant + Secure in an Evolving Landscape

INTRODUCTION

The insurance industry—along with many others—has been forced to evolve over the last year and a half. The pandemic has made digital transformation a necessity to grow along with changing customer needs.

This has led many insurance companies to expedite a trend that started prior to 2020. Insurance companies are expanding their offered services to include features and services that were traditionally offered by financial institutions. This includes:

- Addressing aspects of investment portfolios
- Accepting deposits
- Underwriting debt swaps
- And more

Many of these expansions were the product of necessity. The financial catastrophe of the late 2000's forced many to look at how they dealt with money, as well as the role the government should play in regulating these tactics. This pushed an increase in how finances and customer data were regulated.

However, there are plenty of insurance companies that haven't taken on these expanded roles relating to financial services. These companies still need to consider how government regulations relate to their business. Government requirements are constantly evolving to meet the developing challenges associated with technological advancements and consumer behavior.

Every insurance company needs to be literate in the requirements of government regulations and how they specifically relate to their company.

We'll explore these 6 essential considerations relating to regulatory compliance for the insurance industry:

1. The Impact of Digital Transformation
2. Know Your Regulations
3. Initial Steps to Take
4. Data Security Requirements
5. Tools to Keep You Compliant
6. Staying Updated

01

The Impact of Digital Transformation

Insurance companies have been working for years to find ways to create and improve digital interactions with their customers. This includes a heavy reliance on Salesforce DevOps processes as well as gathering and interpreting relevant data.

Customer service can be improved through properly utilizing customer data. These insights can also make processes more efficient. And all of this is possible through introducing a data governance plan and refining it over time.

One major aspect of digital transformation is the introduction of automation wherever possible. This could be in the DevOps pipeline itself, or even in the use of artificial intelligence dealing directly with customers.

Data-driven technology is only as useful as the data at its disposal. However, insurance companies need to be intentional and careful with how this information is gathered, stored, and used.

HOW THIS RELATES TO COMPLIANCE

Gathering and storing data will be subject to a variety of privacy laws, depending on where your insurance company is located. For instance, those in Europe will need to remain in compliance with the General Data Protection Regulation (GDPR), while companies in America might be subject to rules stipulated by the New York Department of Financial Services (NYDFS) or the California Consumer Privacy Act (CCPA).

Properly handling, securing, and storing sensitive consumer data is at the heart of these regulations. Adherence to the specific rules of each governing body will need to be considered when putting together a data governance plan as well as a data security strategy.

> *"I work as a senior developer for my company and I had awesome experience using this tool. In particular, I liked the features related to easy commit, Dataloader pro and CI Jobs.!"*
>
> JETHA RAM

02

Know Your Regulations

It's very difficult to remain in compliance with regulations if you aren't aware of them. A complete and reliable data governance strategy and data security plan might hit some of the requirements, but it's unlikely to hit them all. Here are a few of the largest government regulations that impact the insurance industry.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is an American statute aimed at regulating how sensitive data is handled in healthcare and adjacent industries—including insurance. There are five main rules of HIPAA:

1. ***Privacy Rule:*** Protects sensitive customer information
2. ***Security Rule:*** Defines the standards for protecting, storing, and using sensitive information
3. ***Transactions Rule:*** Stipulates proper handling of medical records
4. ***Identifiers Rule:*** Defines entities that utilize regulated records
5. ***Enforcement Rule:*** Identifies the rules and consequences of failure to adhere to regulations

GDPR

The General Data Protection Regulation (GDPR) is a European Union regulation that addresses the transfer of personal information between any company—regardless of geographic location—and a European entity. The GDPR grants six rights to consumers:

1. ***Data Access:*** The right to know if a data controller is processing their data
2. ***Right to Object:*** The right to object to their data being processed
3. ***Data Rectification:*** The right to ask to have inaccurate data corrected
4. ***Restriction of Processing:*** The right to request to stop access/processing of their data
5. ***Data Portability:*** The right to ask for a copy of their data so it can be transmitted to another company
6. ***Right to Erasure:*** The right to request to delete or remove their personal data—also known as the "Right to Be Forgotten"

GLBA

The Gramm-Leech-Bliley Act (GLBA) stipulates regulations for financial institutions as well as related businesses (such as insurance companies) regarding the handling of their customers' sensitive personal data. The GLBA is a federal data privacy law that is enforced by state insurance laws for the insurance industry. Some states such as California have expanded the privacy requirements of GLBA with their own data privacy laws.

03 Initial Steps to Take

1. Determine the Applicable Regulations

The regulations that apply to your specific company will be determined by your location as well as the location of those you do business with. For instance, the GDPR is a European regulation, but it also applies to companies in America that do business with entities in the EU. Research federal regulations as well as those in your area.

2. Take Inventory of Your Data

Search through your data to identify areas that are likely to be included in government regulations. This includes personally identifiable information (PII) for your customers, financial data, and more. Classifying sensitive and protected data allows you to focus your efforts on applicable areas instead of spreading your efforts too broadly.

3. Institute Data Governance Policies

Put together a data governance team to oversee the classification and protection of your sensitive information. This team will institute and perform various practices and principles that will maintain the integrity of this important data.

4. Implement Data Security Tools

Proper attention from team members will help your insurance company remain in accordance with government regulations, but powerful tools are still needed to ensure you remain compliant. For example, a data backup and recovery tool protects sensitive data and can be configured to retain this information for specific amounts of time.

5. Data Security Requirements

The various regulations will have different requirements relating to how sensitive information is to be handled. However, there are some overarching considerations that are addressed by these regulations in one form or another. Being aware of these general topics of consideration will help you frame your approach to data security and how it relates to regulatory compliance.

Data Access Safeguards

There must be layers of security in place to properly protect sensitive information. A data breach doesn't necessarily mean the company will be penalized, but a failure to prove intentional security methods can lead to consequences

Accountability After Breach

The insurance company needs to notify anybody with information that was compromised in the event of a data breach. This allows the affected individual to prepare themselves and take extra precautions with their data. The company must then also perform an investigation to figure out how the breach occurred and identify ways to protect against it in the future.

Protect All Information in the System

Customers and clients aren't the only people with sensitive information in your system. Your employees also trust the company to protect their personal data such as PII and financial information. This data must be protected as vigorously as you protect the data of your customers. Government regulations apply to all the data present within your system.

04

Tools to Keep You Compliant

> *Fantastic tool to implement CI/CD concept in Salesforce. The best part is end-to-end automated process for building, packaging, and test execution for Salesforce applications."*
>
> JASVINDER SINGH

We briefly mentioned how tools can help insurance companies remain compliant with various government regulations. These tools must be integrated with your daily processes to stay on top of growing data sets and ensure they are properly protected and addressed. Here are a few types of tools that can help in this effort.

Reporting

Metrics are essential for assessing success in many areas, including data security. Utilizing the reporting capabilities of an Automated Release Management system can provide information on how your data is being accessed. Any unauthorized users can be found and protected against before a data loss event occurs.

Data Backup & Recovery

Insurance companies need to be prepared for every possible scenario. And unfortunately, data loss events are a possibility even when you stay on top of data security concerns. A reliable data backup ensures that your sensitive information won't be lost should something as innocuous as a team member error or natural disaster lead to a data loss event.

Encryption

Cybercriminals are always looking for ways into the system of companies that deal with sensitive information. Encrypting this sensitive information further protects it and adds another layer of security to your customers' data. This extra protection can be the difference between exposing large sets of PII and containing a data breach before it gets out of hand.

Static Code Analysis

Your applications and updates will likely address and contain sensitive customer information. Improperly coded applications create data security vulnerabilities. Ensuring high quality code is a baseline defense against data breaches. Static Code Analysis tools such as AutoRABIT's CodeScan provide real-time visibility into code health so an error never makes it to the deployment stage.

05

Staying Updated

Government regulations are not static. They are continually updated to reflect the changing needs of the industries they impact and the customers they represent. The best way to stay on top of these continuous changes is to monitor the agencies that stipulate the regulations. Here are a few governing bodies in the United States that stipulate regulations relating to the insurance industry:

The Federal Reserve

The Federal Reserve is the central banking agency for the US and has regulatory power over private banks. Insurance companies that have started offering services previously offered by financial institutions will need to pay attention to regulations relating to these matters.

NAIC

The National Association of Insurance Commissioners (NAIC) consists of insurance regulators from all 50 states of the US. This governing body establishes best practices and standards for the insurance industry. They also conduct regulatory oversight. Stay apprised of any recent news from the NAIC.

FINRA

The Financial Industry Regulatory Authority (FINRA) regulates brokerage firms and exchange markets. This is another regulatory body that isn't going to apply to every insurance company. However, companies that provide financial services will need to pay attention. FINRA monitors distribution to protect investors.

SEC

The Securities and Exchange Commission (SEC) is an independent agency within the US federal government. Their main goal is to protect the public against market manipulation. The insurance industry's payouts and other securities are susceptible to SEC regulations.

> *AutoRABIT has helped us add a lot of automation to our software development lifecycle. I highly recommend it!"*
>
> FOREST COOK

CONCLUSION

The insurance industry has expanded to offer new services and interact with customers in new ways. These expanded offerings are directly addressed by government regulations. It's the responsibility of every insurance company to update themselves as to the regulatory requirements that apply to them.

These requirements will vary depending on the specific services your business offers and where you are located. These requirements will continue to be updated so it's in your best interest to follow the governing bodies and stay abreast of any new requirements. A failure to do so can be met with stiff penalties and fines.

Data security is at the heart of these regulations. Utilizing a secure Salesforce DevOps platform sets the groundwork for a properly secure system. Data backups and other tools are essential to achieving this goal. The actions and constant attention of your team members are also required to properly address these needs.

The insurance industry provides important services to their customers. Sensitive information is central to adequately providing these services. Protect this information according to government stipulations and remain in compliance with applicable regulations.

ABOUT

autorabit

AutoRABIT is a Continuous Delivery suite for SaaS platforms. We automate and accelerate the entire application development and release process. This enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. We help enterprises achieve higher release velocity and faster time-to-market.

AutoRABIT provides automated Metadata Deployment, Version Controlling, Advanced Data Loading, Orgs and Sandbox management, Test Automation, and Reporting. Our services complement and extend Salesforce DX. AutoRABIT Vault—our backup and recovery solution—streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery, and endpoint data protection on the Cloud. CodeScan provides full visibility into code health from the first line written through final deployment into production.

VISIT US TODAY TO LEARN MORE

www.autorabit.com

★★★★☆ G2 CROWD