June 2025

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of June 2025 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Insurance Regulatory and Development Authority of India

Maintenance of Information by the Regulated Entities and Sharing of Information by the Authority Regulations 2025

Introduction to the regulation

The Insurance Regulatory and Development Authority of India (IRDAI) has implemented significant regulatory updates aimed at modernizing the insurance sector. Among these is Maintenance of Information by the Regulated Entities and Sharing of Information by the Authority Regulations 2025, which came into effect on January 01, 2025.

As elaborated in **Section 2 of the Regulations**; the key objectives of this regulation is to enable Insurers to maintain data as required for its operations in electronic form; to ensure security and compliance with applicable laws; and to adopt an established data governance framework.

From a technology and governance perspective, this regulation puts emphasis on -

- **Enhanced focus on digital infrastructure:** Regulated entities (REs) will need to invest in robust IT infrastructure and systems to ensure compliance with the mandate for electronic record-keeping and data storage within India.
- **Strengthened data governance:** Implementing a board-approved data governance framework will require a comprehensive review of existing data management practices and the establishment of new policies and procedures.
- **Improved security measures:** The emphasis on stringent security and privacy measures necessitates a proactive approach to cybersecurity to protect policyholder and claim data.
- **Greater transparency and accountability:** The clear guidelines for information sharing will promote greater transparency and accountability in the sector.

In essence, the message is a directive for regulated entities to ensure robust, secure, compliant, and transparent data management practices, to support operations, policyholder interests, and regulatory oversight.

June 2025

An **IRDAI Regulated Entity** (Sec 3.x of the Regulation), may use Google Cloud products and services as part of their operations. Here, we'll discuss how Google Cloud as a cloud service provider can help the REs meet their obligations per this guideline.

Frequently Asked Questions

1. **Who does this regulation mainly apply to? What is Google Cloud's role in this?**
   This regulation applies to the regulated entities of IRDAI **(as listed in Section 3.x of the Regulation)** and not directly addressed to cloud providers or outsourcing companies. As a cloud service provider,Google Cloud provides a secure platform with configurable capabilities that can be used by the regulated entities, to meet the obligations per this regulation.

2. **Are there any restrictions on the use of cloud service providers by IRDAI regulated entities for their various organizational needs?**
   No, this regulation does not prohibit or restrict the use of cloud services.
   Regulated entities can configure the services listed at Google Cloud Platform Services with Data Residency in a way that data, such as insurance records or minimum information as described under the regulation, are stored at rest within India regions. The list of services and the data region details can be understood in more detail here.

3. **How does Google ensure securing its own infrastructure?**
   Google manages the security of its infrastructure which includes hardware, software, networking, and facilities that support the services. We provide detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. Key resources for REs:

   - Trusted Cloud infrastructure
   - Google Security overview
   - Cloud-native security
   - Infrastructure security design overview
   - Security resources

4. **What are some security measures REs can implement to secure data and applications in Google cloud**

   REs need to define the security of their data and applications in the cloud. This refers to the security measures that REs choose to implement and operate when they use Google Cloud Services.

We encrypt data in transit between our facilities and at rest, ensuring that it can only be accessed by authorized roles and services with audited access to the encryption keys. Our key security documentation provides details on how we safeguard customers' data and secure our platform and infrastructure.

In addition to the other tools and practices available to you outside Google, you can choose to use products and tools offered by Google to enhance and monitor the security of your data. We also publish guidance on security best practices, security use cases, and security blueprints.

5. **How can Google Cloud enable REs to ensure insurance records are stored within India?**
   Google Cloud offers customers the ability to control where your data is stored. Customers may configure the services listed at Google Cloud Platform Services with Data Residency to store insurance records and minimum information, which is the focus of this regulation in **Mumbai (asia-south1) or Delhi (asia-south2)**, and Google Cloud will store that customer data at rest only in the selected region/multi-region in accordance with our Service Specific Terms.

   With Cloud IAM configuration, customers can prevent employees from accidentally storing data in the wrong Google Cloud region. To assist customers in enforcing these controls, Google Cloud offers organization policy constraints, which can be applied at the organization, folder, or project level. Customers can limit the physical location of a new resource with the organization policy service resource locations constraint.

Google Cloud runs on a technology platform that is designed and built to operate securely. Google Cloud regularly undergoes independent verification of its security, privacy, and compliance controls, and receives certifications, attestations, and audit reports to demonstrate compliance. For a complete listing of our compliance offerings, see the compliance resource center.

Our strong contractual commitments help you maintain control over your data. Google recognizes that IRDAI regulated entities and their supervisory authorities must be able to audit our services effectively. Google grants information, audit and access rights to regulated entities, supervisory authorities, and both their appointees. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity.

The protection of your data is a primary design consideration for our infrastructure, products, and operations. Protecting data is core to our business, so we make extensive investments in security, resources, and expertise at a scale.