ManipalCigna Health Insurance Company Limited

Anti-Fraud Policy

Owner: Fraud Monitoring Unit

Approver: ManipalCigna Board of Directors

Version: 1

Effective Date: 01st April 2026

Review History

Date of Review	Changes to Section	Review initiated by	Review signed off by	Review Approved by	Version Number	Effective from
NA	New Policy	Fraud Control Unit	Chief Compliance and Governance Officer	Board	1.0	1st April, 2026

Confidentiality Clause:

All information held about the procedure or in connection with the procedure and any of the above is to be regarded as confidential. One will not at any time during tenure of employment or afterwards, disclose to any person any information as to the business, dealings, practice, accounts, finances, trading, software, know-how, affairs of the procedure or otherwise connected with the procedure. Any breach of this clause would constitute very serious disciplinary action.

Table of Contents

1. Introduction

This Anti Fraud Framework and Policy (" Policy") is created considering the nature of business, size, risk profile, overall business strategy, products, distribution channels, technology infrastructure, with the objective to o deter, prevent, detect, report and remedy fraud risks effectively. It establishes a foundation for promoting ethical conduct, accountability, and transparency across all operations. Through clearly defined principles, processes, and controls, the framework ensures that fraud risks are identified, assessed, and mitigated in a consistent and effective manner.

This Policy strengthens the organization's resilience by minimizing exposure to fraud-related incidents and enabling a swift and coordinated response when issues arise. Through active participation from leadership, employees, and stakeholders, the framework helps safeguard organizational resources and reinforces trust in its operations.

IRDAI vide its circular no IRDA/IID/GDL/MISC/112/10/2025 dated 9th 2025 has issued guidelines to provide regulatory framework on measures to be taken by Insurers and Distribution Channels to address and manage risks emanating from fraud. The aforesaid guidelines upon coming to effect on April1, 2026 shall repeal the Insurance Fraud Monitoring Framework issued vide ref: IRDA/SDD/MISC/CIR/009/01/2013 dated 21st January 2013. Accordingly the existing the Anti-Fraud Policy and Framework of the Company will be replaced by this Policy and will be effective from 1st April 2026. Anything done or any action taken or purported to have been done or taken in respect of the repealed Insurance Anti-Fraud Policy shall be deemed to have been done or taken under the corresponding provisions of this Policy.

1.1 Scope and Applicability

ManipalCigna Health Insurance Company Limited (herein after referred to as "The Company") shall place high emphasis on prevention, detection, Control and deterrence through below mentioned elements

- Create an environment and culture of honesty and high ethics through fraud risk and control
- Implementation of processes, procedure and controls to identify, assess and mitigate fraud risk and reduce the opportunity of fraud

This Policy shall be applicable to all employees, contractual staff of the Company as well as the agents, distribution channel partners, intermediaries, vendors, contractors, consultants, policy holders, third parties,Third Party Administrators, effective from 1st April 2026.

The FMU will be independent from Internal Audit, to support the FMC in discharging its functions and effective implementation of measures suggested by the FMC.

This policy should be read in conjunction with applicable policies of the Company like Code of Conduct, AML policy, Risk management policy, Whistle blower policy, Fraud Monitoring Framework and Policy and Information Security and Cyber Security policy.

1.2 Objectives

To establish a comprehensive framework in order to deter, prevent, detect, report and remedy fraud risks effectively across the Company. These guidelines aim to enhance the sector's resilience against fraud, foster a culture of integrity, protect policyholders' interests, safeguard financial stability and maintain public trust.

1.3 Key Terms Used

- IRDAI – Insurance Regulatory & Development Authority of India
- TPA – Third Party Administrator
- FMU – Fraud Monitoring Unit
- FMC – Fraud Monitoring Committee
- CGO – Chief Governance Officer
- RMC – Risk Management Committee
- F&I – Fraud and Investigation
- IIB – Insurance Information Bureau

2. Definition of Fraud

IRDAI vide its circular no IRDA/IID/GDL/MISC/112/10/2025 dated 9th October 2025 defined the following terms:

(i) Insurance Fraud means an act or omission intended to gain advantage through dishonest or unlawful means, for a party committing the fraud or for other related parties; including but not limited to:
- Misappropriating assets
- Deliberately misrepresenting, concealing, not disclosing one or more material fact relevant to the financial decision, transaction or otherwise
- Abusing responsibility, position of trust or fiduciary relationship.

(ii) Red Flag Indicator means a possible warning sign, that points to a potential fraud and may require further investigation or analysis of a fact, event, statement, or claim, either alone or with other indicators.

(iii) Cyber or New Age Fraud means any insurance fraud carried out using digital or new age technologies.

(iv) Distribution Channels shall have the same meaning assigned to it under sub clause (8) of clause 5 of IRDAI (Protection of Policyholders' Interests and Allied Matters of Insurers) Regulations, 2024.

2.1 Classification of Fraud

Fraud can be broadly categorised into the below mentioned categories

(i) **Internal Fraud**: Fraud/ misappropriation against the Company involving its Director, Manager and/or any other officer or staff member (by whatever name called)
(ii) **Distribution Channel Fraud**: Fraud involving distribution channels.
(iii) **Policyholder Fraud and/or Claims Fraud**: Fraud involving any person(s), in obtaining coverage or payment during the purchase, servicing, or claim of insurance policy.
(iv) **External Fraud:** Fraud involving external parties' / service providers / vendors etc**.**
(v) **Affinity Fraud or Complex Fraud:** Fraud involving collusion among one or more fraud perpetrators in the above categories

2.2 Zero Tolerance Policy

The Company has adopted Zero tolerance policy for fraudulent activities or attempts to commit a fraud and prompt & strict action shall be taken against perpetrators and/or personnel attempting to conceal instances of fraud.

2.3 Governance

The Company shall follow high standards of integrity and honesty by encouraging transparency and openness at all levels of hierarchy to prevent fraud or concealment of fraudulent practices.

Regular communication for creating awareness amongst employees, policy holders, and the general public will be maintained through training programmes, emailers or through any other appropriate forums

3. Anti-Fraud Framework

Anti-Fraud Framework lays down the key activities for, identifying, and process of investigation, timelines to be adhered while investigating, monitoring and reporting of Frauds, committed or suspected fraudulent activities by internal and external stakeholders such as employees, directors network hospitals, distribution channels, TPA, external vendors, policyholders etc. The Anti-Fraud Policy forms part of the Fraud Monitoring Framework of the Company.

3.1 Fraud /Suspected Identification and Monitoring.

The primary responsibility of fraud prevention lies with the respective department heads, and they are the first line of defence and responsible for implementation of appropriate control measures for prevention of fraudulent or suspected fraudulent activities.

Department Heads will inform his team members that the company has a Zero Tolerance Policy for fraud activities and educate them to report any illegal or fraudulent activity. Department heads will report immediately any instances of any attempted, suspected or confirmed fraud to the email ID listed in Annexure 2 along with available supporting documents.

All the employees/officers of the Company have the responsibility to inform about any fraud or suspected fraudulent activity to their reporting managers or to the email ID listed in Annexure 2.

The distribution channels, TPAs, Vendors and third parties are responsible to inform about any fraud or suspected fraud activity to their report managers or to the email ID listed in Annexure2.

FMU will enable coordination with the respective department heads as may be required for investigating the suspected fraud to seek additional information and documentation. FMU will evaluate and classify them into required category of fraud. Prioritize cases based on severity, risk exposure, regulatory relevance, and potential customer impact. Conduct fraud-sensitive audits for compliance with Fraud Risk Monitoring Framework, monitoring vendor activities for compliance with fraud prevention measures and contractual obligations.

Identification and mitigation of claims related Fraud will be primarily carried out by the Claims / F&I team as part of day-to-day claims evaluation/processing and specific trends to be reported to FMU as may be deemed necessary for further investigation.

3.2 Investigation Process & Turnaround Times (TATs)

The following action shall be taken in response to an alleged or suspected incident of fraud reported

- Logging of case: FMU will maintain a repository/ register of the reported cases.
- Preliminary Inquiry: Upon logging of the case, FMU will carry out preliminary inquiry on the following lines.
  - Classification of Fraud Category (Internal, Distribution Channel, Policyholder, External, Affinity /Complex, etc.)
  - Review of available information / documents
  - Calling for additional information / documents
  - Deciding the methodology of assessment / investigation (Internal* / External#)
  - Review the findings

- Referring to FMC, if any fraud or suspected fraudulent activity with all the relevant documents.

- Role of FMC
  - Review the facts and findings submitted by FMU for review.
  - Recommending action as may be required**^**

^ Incident Matrix to be used for reference for recommending action (Refer Annexure 3)

*****Internal Investigation – This type of investigation refers to the investigation undertaken by the authorized officials of the Company

For the purpose of internal investigation, the members of the investigation team will have

a. Free and unrestricted access to all Company records (including emails, folders and files) and premises whether owned or rented.
b. Authority to examine, copy and/or remove all or any portion of the contents of records without prior knowledge or consent of any individual who may use or have custody of any such items.
c. Authority to call / meet on request any party (Internal/External) in connection with fraud or suspected fraud cases

#Verification / Investigation by External Agency- Depending on the gravity / nature of the case, FMU may assign the case to an external agency for verification / investigation as per process / necessary approvals. Such an agency will conduct the verification / investigation and submit its report along with the findings and necessary evidence.

Turnaround Times (TAT)

Investigation shall be completed within the timeframe as specified from time to time. For large frauds involving a number of people or where the financial impact / complexity of frauds is high the investigation timeline may be extended appropriately. Conclusion of the investigation should be documented.

• Logging: FMU registers cases within and updates the register on the same day or next day of receipt of complaint.
• Preliminary assessment: within 7 business days (classification, evidence collection, method – internal/external).
• Investigation: conclude within 45 calendar days for standard cases; within 60–90 days for complex cases; in case of extensions the same to documented and approved by FMC

3.3 Reporting

Reporting will be done as per the Fraud Monitoring Framework and Policy.

The Whistle Blower complaints shall be handled as per the Company's Whistle Blower Policy, which includes Whistle Blower protection,

If the case requires any involvement of any law enforcement agency or legal matters, then the Legal & Compliance team will be involved for necessary action. CGO will present an update on Anti- Fraud Framework to the Audit / Risk Management Committee of the Board on quarterly basis or earlier as deemed necessary.

Fraud Monitoring report is submitted to the regulator in the specified format after the closure of financial year. Format available in Annexure 1

3.4 Monitoring

The Department Heads i.e. the First line of Defence will continue to monitor the activities of the department and exercise necessary controls from a fraud mitigation perspective. FMU team may undertake periodic reviews as a part of monitoring process as described in the Fraud Monitoring Framework.

4. Review of the Policy

- To ensure compliance with the regulatory guidelines, the Anti-Fraud Policy shall be reviewed at least once in a year and changes if any submitted to the Board of Directors for approval.
- In view of modifications to regulatory requirements, suitable addendums should be issued within the company to communicate the revised guidelines.

5. Annexures

Annexure 1 - IRDA Circular

Particulars	Attachment
IRDA/IID/GDL/MISC/112/10/2025 , 9th October 2025	IRDAI (Insurance Fraud Monitoring Fra

Annexure 2 - Contact Person

Name	Designation	Email ID
Deepak Yadav	Senior Manager- Fraud Control Unit	fmu@manipalcigna.com
Sangeeta Menon	DVP-Legal and Fraud Control Unit	fmu@manipalcigna.com

Annexure 3 - Incidents Matrix

Particulars	Attachment
Incident Matrix	Incidents Matrix.xlsx