national health authority
सत्यमेव जयते

भा बी वि वि प्रा
irdai

IRDAI-NHA JOINT WORKING GROUP

Report of Sub-group on Fraud Control

IRDAI-NHA
JOINT WORKING GROUP

Report of Sub-group on Fraud Control

Table of Content

IRDAI Order- Constitution of Joint Working Group

भारतीय बीमा विनियामक और विकास प्राधिकरण
INSURANCE REGULATORY AND
DEVELOPMENT AUTHORITY OF INDIA

Ref: IRDAI/HLT/ORD/Misc/37/03/2019 Date: 05.03.2019

ORDER

Re: Constitution of Joint working group of IRDAI and NHA

Government of India has launched Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (AB-PMJAY) for providing secondary and tertiary care cashless treatment at empanelled private and public hospitals across the country to families listed in SECC (Socio-Economic Caste Census) 2011.To support the Implementation of AB-PMJAY with the active involvement of various stakeholders and to further strengthen the health insurance ecosystem it is desired that IRDAI and NHA work on key areas of mutual interest and cooperation.

In order to work in this direction, a Joint Working Group is constituted with the following Members:

1. Dr Dinesh Arora, Dy. CEO,NHA , Chair
2. Mr. Suresh Mathur, ED, IRDAI, Co- Chair
3. Mr. Kunnel Prem, CEO, IIB, Member
4. Ms.Yegnapriya Bharath, CGM, IRDAI, Member
5. Mr. A.V. Rao , G M, IRDAI, Member
6. Mr. D V S Ramesh, G M, IRDAI, Member
7. Dr Arun Gupta , ED,NHA, Member
8. Mr. Kiran Anandampillai, Advisor, NHA, Member
9. Mr. Nishant Jain, Advisor, NHA, Member
10. Ms. Malti Jaswal, Advisor, NHA, Member
11. Dr Pankaj Sharma , Manager, IRDAI , Member-Convener

Terms of reference for the Joint Working Group shall be: -

1. **Network hospitals management:** To have a National Repository of Empanelled Hospitals under Insurance/Government schemes with defined standards for quality and package rates and codes.
    i. Defining Hospital infrastructure and Facility Audits to understand capacity of Hospitals, Specialists availability.
    ii. Developing a roadmap to get one Common list of Accredited/ Verified hospitals for the entire Industry including ROHINI, NHRR, NIN and PMJAY Databases.
    iii. Comparative Study of Packages and their rates and mapping to uniform codes.
    iv. Defining Standards and Indicators for safe and quality Healthcare to Patients.

    Timeline: 12 months

सर्वे नं. 115/1, फाइनेंशियल डिस्ट्रिक्ट, नानकरामगुडा, हैदराबाद-500 032, भारत
फोन : +91-40-2020 4000 वेबसाइट : www.irdai.gov.in
Survey No. 115/1, Financial District, Nanakramguda, Hyderabad-500 032, India
Phone : +91-40-2020 4000 Website : www.irdai.gov.in

2. **Data Standardization and exchange:** To create standard data formats across Health Insurance payers for analysis and policy making.

    i. Developing standardized data tables to capture and report the data, identifying data elements common with IRDAI and PMJAY.

    ii. Setting up a framework for capturing and exchanging data.

    Timeline: 3 months

3. **Fraud and abuse control:** To help detect and deter frauds through common repository and capacity building.

    i. To develop a standard reporting format for fraud and abuse to be used across the industry and Govt. Schemes.

    ii. Repository of fraudulent transactions, modus operandi and entities.

    iii. Develop standards for field verification and investigation.

    iv. Develop "name and shame" guidelines.

    Timeline: 6 months

4. **Common IT infrastructure for health Insurance claims management:** To Increase service efficiency and transparency amongst stakeholders in delivery of Health Insurance services.

    i. Defining the roadmap for electronic, paperless, codified data exchange between payer and provider, collation and analysis

    ii. Defining a roadmap for creation of standard electronic personal health record for insured population with a common identifier.

    Timeline: 6 months

The working group may hold meetings as and when needed and submit a report with recommendations within the timelines prescribed. The working group may consult experts from the Insurance Industry, Healthcare Providers, NABH, IT, Third Party Administrators etc. in the course of their deliberations..

Sujay Banarji
Member

I. Composition of Sub-Group on Fraud Control

Chair: Ms. Malti Jaswal, NHA

Members:

1. Ms Yegnapriya Bharath, IRDAI
2. Mr Kunnel Prem, IIB

Co-opted non-Members and Special Invitees

1. Ms Geetali Tare, NHA
2. Mr Jagdeesha Reddy, IIB
3. Mr Shivakumar Shankar, LexisNexis
4. Ms Parul Naib, NHA
5. Mr Sashi Nair, GI Council
6. Dr. Arun Gupta, NHA
7. Mr DVS Ramesh, IRDAI
8. Mr Surendra Tiwari, NHA
9. Mr Rohit Jha, NHA
10. Dr Chander Mohan Asrani, NHA
11. Dr Satya Bhushan, NHA
12. Dr Ankita Chaubisa, NHA
13. Dr. Bhabatosh Mishra, Apollo Munich Health Insurance
14. Dr Sudhalakshmi D, Apollo Munich Health Insurance
15. Mr Vinay Verma, Oriental Insurance Company
16. Mr Chandrakant Mishra, Religre Health Insurance
17. Dr. Amit Gupta, Religare Health Insurance

II. Executive summary

The Launch of Ayushman Bharat - Pradhan Mantri Jan Arogya Yojana PMJAY) by Hon'ble Prime Minister on Sept 23rd 2018 has brought over 50 crore vulnerable Indians into the fold of healthcare financial risk protection. National Health Authority (NHA) is the nodal agency for implementation of the Scheme. Together with private paid health insurance organized under the aegis of Insurance Regulatory & Development Authority of India (IRDAI), more than 50% of Indian population now stands covered, a significant step towards achieving Universal Health Coverage. World over healthcare schemes and insurance programs are prone to integrity violations due the very nature of healthcare - asymmetry of information, provider induced demand and malpractices, ghost policy holders, fake beneficiaries etc. with serious implications for health outcomes besides financial waste.

As payers and custodians, IRDAI and NHA have set up a Joint Working Group (JWG) to look into areas of mutual cooperation which will help improve eco-system of health insurance, bringing in best practices and greater efficiency, effective collaboration etc. One of the sub-groups under JWG was tasked with key deliverable 'to help detect and deter frauds through common repository and capacity building' and specific sub-components as below:

1. Develop a standard reporting format for fraud and abuse to be used across the industry and Govt. Schemes.
2. Develop a Repository of fraudulent transactions, modus operandi and entities.
3. Develop standards for field verification and investigation.
4. Develop "name and shame" guidelines.

This Report is the result of work accomplished by the sub-group and provides following recommendations:

a) The definition of fraud and abuse should be standardized as per Report across eco system of health insurance/assurance schemes. Confirmation of a suspect transaction/event as 'fraud or abuse' should be done by concerned Payer after due-diligence and investigation.

b) All contracts signed by a Payer - with policy holder, empaneled hospital, intermediary, employee etc. should mandatorily incorporate standard definition of fraud and standard clauses as listed in

Report to enumerate the repercussions of committing fraud, range of punitive actions that may ensue.

c) Repository of fraudulent transactions, modus operandi and entities involved should be maintained at General Insurance Council (GI Council) level for insurance industry and at NHA level for PMJAY and all other Govt schemes. It should also include action taken by Payer.

d) Every Payer should be mandated by its governing authority i.e. IRDAI and NHA, to report both - suspect and confirmed frauds to respective Repository on fortnightly basis. In due course the data sharing should be done through APIs directly.

e) Both Repositories should have common minimum data points as suggested in the Report for data sharing, drawing of MIS, reports etc. and to develop 360* view of fraudulent parties, risk profiling, analysis of types of fraud and fraud Heat map of India across spectrum of Payers.

f) Standards for field investigation should be adopted with minimum common data/information as per Report both for private paid health insurance and PMJAY/Govt schemes.

g) A common talent pool should be created for effective investigation and a Certification program as per Report should be developed for ensuring minimum standards. In due course Certification should be made a mandatory requirement by IRDAI and NHA.

h) Name and Shame guidelines is an area for further development. A conservative approach is presently suggested in the Report in the absence of legal provisions in the country.

i) A strong legal framework needs to be conceptualized which should culminate in enactment of National Health Insurance Anti-Fraud Act by the Government.

j) Further collaboration of sub-group is suggested for implementation of Report, governance and review mechanisms and for covering rest areas in the realm of prevention, detection and deterrence.

III. Background

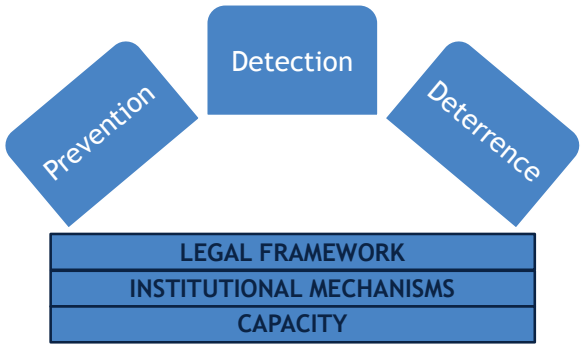
Globally, countries are expanding access to health services and providing financial protection to their citizens through the implementation of national health insurance schemes. Similarly, increasing health awareness in the global population has led to expansion of the private health insurance sector, which has introduced innovative models and schemes to provide cost-effective and efficient health insurance cover to corporate employees, general population and vulnerable groups.

While the strategies, policies, and technologies used to support these health insurance schemes are as varied as the participants implementing them, one common challenge is continuously cited — the increasing risk of fraud and abuse leading to leakage and wastage of funds allocated for healthcare benefits[1]. As per the Global Health Care Anti-Fraud Network, it is estimated that $260 billion (180 billion euros)—or approximately 6% of global health care spending—is lost to fraud each year[2]. World over healthcare schemes and insurance programs are prone to integrity violations due the very nature of healthcare - asymmetry of information, provider induced demand and malpractices, ghost policy holders, fake beneficiaries etc. with serious implications for health outcomes besides financial waste.

With launch of Ayushman Bharat - Pradhan Mantri Jan Arogya Yojana (PMJAY), the total number of people covered under health insurance – private paid, organized through insurance companies under the aegis of IRDAI or Govt funded, organized by State Govts (with or without involving insurance mode) under the aegis of NHA now stands at approximately 65 crores – 15 crores under private paid insurance, and 50 crores under PMJAY, i.e. more than 50% of Indian population now stands covered. This does not include people covered under schemes like CGHS, Armed Forces etc. The total number of claim transactions (primarily in-patient hospitalization episodes) collectively generated by the covered population shall exceed 2.5 crores per annum in very near future. The estimates of leakage due to fraud and abuse vary for different products/schemes/territories and it is also difficult to quantify the same due to the very nature of healthcare services. More importantly, the impact of healthcare fraud is not only financial but also, on people's health which is a grave concern. As the coverage/penetration of health insurance expands to more people, for more services, the element of fraud and abuse will also to go up exponentially if handled inadequately.

[1] Determining Common Requirements for National Health Insurance Information Systems, January 2012
[2] The Challenge of Healthcare Fraud- NHCAA: https://www.ghcan.org/global-anti-fraud-resources/the-health-care-fraud-challenge/

The anti-fraud conceptual framework rests on 3 pillars:



Source: Toolkit for Tackling Error, Fraud, and Corruption in Social Protection Programs

For PMJAY, the framework has been enshrined in Anti-fraud Guidelines 2018 (refer Annexure I) and the same is being operationalized by National Anti-Fraud Unit (NAFU) of NHA and State Anti-Fraud Units (SAFU) in the implementing States. In 2013, IRDAI introduced the Fraud Risk Monitoring Framework (refer Annexure 2) for the insurance industry, to be complied with all insurers mandatorily. The players in insurance industry have also adopted the framework – both at policy and operational level. It remains mostly at individual company level with limited collaborative action across the industry. The institutional frame work for anti-fraud needs strengthening across board It is also to be noted that legal framework for anti-fraud is relatively an under developed area in India with no specific law dealing with healthcare fraud or insurance fraud which would lay down stringent punitive and deterrent provisions to deal with fraudsters.

To develop a strong and efficient fraud mitigation strategy, it requires dedicated commitment of all stakeholders including the government, state agencies, insurers and their intermediaries as well as the beneficiary community. In the above background, it is imperative that IRDAI and NHA should join hands and collaborate for effective measures to fight fraud and abuse in healthcare protection schemes/insurance products for overall betterment of health insurance ecosystem in the country. Thus, one of the Sub-groups under Joint Working Group was assigned to work on this important area. Also, it is the 'payer' role, which is common, it does not matter whether PMJAY is being implemented in a particular State under Trust model, insurance model or hybrid model, i.e. health insurance and assurance both are covered.

IV. Deliverables

From the vast canvas of 'detection, prevention and deterrence' of fraud and abuse, the present deliverables of Sub-group are confined 'to help detect and deter frauds through common repository and capacity building'. For this purpose, following sub-components have been further defined so that an operational level collaboration can take-off in a short period of time.

1. Develop a standard reporting format for fraud and abuse to be used across the industry and Govt. Schemes.
2. Develop a Repository of fraudulent transactions, modus operandi and entities.
3. Develop standards for field verification and investigation.
4. Develop "name and shame" guidelines.

The Draft Report is the result of work accomplished by the Sub-group on above pre-defined areas.

1. Standard reporting format for fraud and abuse to be used across the industry and Govt. Schemes.

To understand the total impact and quantum of fraud and deal with the same collectively, there is a need for all Payers to report fraud to a central authority or repository in a standard format. However, before developing standard format, it is also important to agree upon following sub-components which are going to be reported:

1.1. Common definition of fraud and abuse, what it constitutes, what it doesn't
1.2. Which are the potential parties involved in fraud
1.3. What are common types of frauds committed by these parties

Payers should also agree upon a common approach to deal with fraudsters by way of standard mandatory clauses/provisions for deterring/mitigating fraud in different contracts. It would also help disseminate knowledge with all stakeholders, especially providers whose continued participation is essential for health insurance/financing mechanisms to work.

1.1. Definition of Fraud and Abuse

Fraud shall mean and include any intentional deception, manipulation of facts and / or documents or misrepresentation made by a person or organization with the knowledge that the deception could

result in unauthorized financial or other benefit to herself/himself or some other person or organization. It includes any act that may constitute fraud under any applicable law in India.

An indicative list of what connotes fraud:

- Impersonation
- Counterfeiting
- Misappropriation
- Criminal breach of trust
- Cheating
- Forgery
- Falsification
- Concealment
- Breach of Contract

What does not connote a fraud – an indicative list

- Errors - un-intentional mistakes during the process of healthcare delivery
- Waste – inadvertent use of resources

Abuse refers to those provider practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. It also includes beneficiary practices that result in unnecessary cost.' Few examples of common health insurance abuse would be - excessive diagnostic tests, extended length of stay and conversion of day procedure to overnight admission, upcoding etc.

The main purpose of both fraud and abuse is financial and non-financial gain. Fraud is wilful and deliberate, involves financial gain, is done under false pretence and is illegal, abuse generally fails to meet one or more of these criteria, hence assumed to be less severe in nature. However, it is recommended that repeated instances of abuse, which continue to be indulged in by the perpetrator despite warnings, should be termed as fraud beyond certain threshold and dealt with in similar fashion as fraud.

Definition of fraud and stakeholders is defined in many international healthcare programs, refer Annexure 3

1.2. Parties involved in health insurance fraud

There are multiple stakeholders in a health insurance program and any of the stakeholders may be involved in committing fraud either individually or jointly with one or more stakeholders.

a) **Healthcare provider -** Common examples:
   - Getting empanelled through manipulation of records or service/facilities etc.;
   - Manipulation of documents/falsification of claims/procedures
   - Billing for services not provided, upcoding, unbundling etc.
   - Accepting kickbacks for patient referrals
   - Upcoding
   - Unbundling
   - Collecting unauthorized fees/money from beneficiaries
   - Concealment of material facts like pre-existing medical history, substance abuse by insured

b) **Beneficiary under PMJAY or a Govt scheme** – Common examples:
   - Making a false statement of eligibility to access health services
   - Knowingly allowing impersonation / identity theft to access health services
   - Engaging in a conspiracy with service providers to submit false claims or make money

c) **Policy Holder under an insurance contract (including employees covered under Group policies)–** common examples:
   - Obtaining insurance coverage through misrepresentation, non-disclosure of facts
   - Making false/exaggerated claims, colluding with providers

d) **Intermediaries like agent, broker, Common Service Centers /Village Level Entrepreneur (for PMJAY) –** common examples:
   - Colluding with policy holder for organizing cover with false documents
   - Facilitating false claims through collusion with policy holder and/or providers
   - Organizing policies in fake names
   - Issuing beneficiary cards with fake documents or names

e) **Payer fraud – Govt. Health Agency, Insurer, TPA**

- Colluding with providers for wrongful empanelment, false claims
- Conniving with beneficiary/policyholders for wrongful claims
- Manipulating beneficiary list/covered members list;
- Withholding/Settling/paying claims for favor/kickbacks

f) **Internal Member –** employees, board members, senior executives

- Colluding with external stakeholders - providers, beneficiaries, intermediaries, policyholders for wrongful claims/insurance covers
- Siphoning of money/funds with or without connivance of external parties

1.3. List of Common types of frauds

Given below is indicative list of common types of fraud for purpose of standard codification at industry level and Fraud Repository

- Billing for services, procedures, and/or supplies not provided
- Unwarranted procedures, diagnostics and services, (classified separately to indicate patient harm or without harm)
- Upcoding, unbundling, (classified separately to indicate patient harm or without harm)
- Manipulating/fudging documents/impersonation to obtain insurance cover/scheme benefit with/without connivance of other stakeholders
- Manipulating/fudging documents/impersonation for claim purpose with/without connivance of other stakeholders
- Acting/colluding for kickbacks/favors

The above list is not to be mistaken for different triggers which are applied at system level based on Rule Engines or at process level by medical team to detect pattern/outlier cases. The triggers are more specific to a Payer, a product or a Scheme, should be customized as per requirements, however underlying fraud should be listed in one or more categories as listed above.

1.4. Confirmation of 'fraud'

It is important to make a distinction between fraud and a suspect transaction/event which may or may not turn out to be fraud. Understandably every fraud shall first be a suspicion which would need to be further probed, investigated and examined along with documentary and circumstantial evidence before being categorized/confirmed as fraud according to standard definition. Due process

of investigation with fair chance given to suspect party is also important from the point of natural justice. After carrying out satisfactory due diligence, it is for the individual payer to confirm a suspect transaction/event as fraud or abuse as per standard definitions, the suggested time limit for same should not exceed 4-6 weeks from the time of detection. The purpose of standard investigation report format is to help payers carry out investigation process in efficient manner.

1.5. Mandatory clauses/provisions under payer-provider contract for deterrence and mitigation of fraud

As one of the key parties involved in health insurance fraud is healthcare provider, the preemptive measures for prevention and deterrence of frauds committed by healthcare providers hold great significance. An important deterrent measure in this context relates to incorporation of legally binding contractual provisions in the Service Level Agreement or MOU signed between payer and provider so that provider is forewarned and understands the consequences of committing fraud. Such contractual provisions exist world over in healthcare programs, refer Annexure 4.

Contractual provisions help prevent and resolve disputes, law suits etc. that may arise out of suspension, de-empanelment and other actions. However, it is equally important to include provisions which protect healthcare provider from prejudicial treatment or harassment by payer/its employees or representatives and facilitate confidential reporting, redressal without fear of retribution or victimization.

It is recommended that such contracts should mandatorily include following clauses for mitigation of fraud committed by a provider, giving the right to payer to carry out all or some actions as need be, though it is preferred all payers across insurance industry and PMJAY/Govt schemes maintain uniformity of action. It is also important for closure of action within a given time frame else it loses its significance; hence timelines are also suggested along with actions. It also sends a strong signal to other providers.

An individual payer - insurance company or State Health Agency or Govt agency may decide severity of punishment and penalties under these clauses as per its own requirements or special circumstances e.g. treatment of public hospitals empaneled under PMJAY/Govt scheme may be different than private hospitals, it may involve dismissal from services of concerned people/doctor rather than de-empanelment of hospital. Or availability of very few empaneled providers in a given

geography for an insurance company or PMJAY, may involve taking positive action like educating provider before show-cause notice, de-empanelment etc. or limiting the penalty amount etc.

The mandatory clauses as per following list should be incorporated in all contracts signed between payer and provider:

a) Standard definition of fraud and abuse
b) List of actions that shall follow on detection of a suspicious transaction/abuse by a provider:
   i. Show-cause Notice/warning letter
   ii. Temporary Suspension
   iii. Payer's right to carry out detailed Investigation, to obtain documentary evidence, to audit hospital's records, to visit premises, interview people etc.
   iv. Report to relevant Repository

Recommended time period for closure of action under this section – 1 month from date of detection.

c) List of actions that shall follow confirmation of fraudulent act by a provider:
   i. De-empanelment and termination of agreement
   ii. Recovery (of amount equal to fraudulent claim/transaction)
   iii. Penalties (punitive recoveries – multiple times of fraudulent transaction)
   iv. Report to relevant Repository
   v. Publication under 'Name and Shame'
   vi. Report under Medical Establishments Act of the State (wherever applicable) and/or to MCI (refer Annexure 8) for reporting different malpractices under relevant sections of MCI)
   vii. Lodging of FIR, especially if fraud involves 'patient harm' (even if it involves lesser financial consequences) or is committed en-masse/over a large number of claims

Recommended time period for closure of all actions under this section – 6 month from date of detection, individual sub-actions may be completed 2 months onwards

d) List of action that shall follow action confirmation of fraudulent act by a provider against 3 insurance companies/payers/schemes
   i. Possible de-empanelment by other payers
   ii. Possible Industry blacklisting - barring the hospital from participating in any payer program in the country

Recommended time period for closure of actions under this section – 9 month

e) List of mechanisms for providers' reporting of issues/concerns e.g. deliberate delay in payment of claim, withholding payment, wrongful issue of show-cause notice etc, in confidential manner if

need be, and fair and timely redressal of same by payer's higher authorities in unbiased manner. Whistle Blower mechanisms should be explained and be available to all stakeholders alike.

1.6. Standard format for reporting

The sub-group recommends that every payer should mandatorily report fraud – both suspect and confirmed to the relevant repository every fortnight. It is to be noted that every fraud shall be reported first as a suspect transaction/event. As explained previously, the categorization as 'confirmed' shall be subsequent to due process of investigation and evidence collection. The suspect transactions which are not confirmed as fraud after investigation due to any reason including weak evidence shall be categorized as 'unconfirmed' and shall remain in the Repository for future reference by Payers. Hence at any given point of time, there shall be 3 categories of listed items – suspect, confirmed and unconfirmed. The Report format shall correspond to the data fields required as per Repository discussed in next section.

2. Repository of fraudulent transactions, modus operandi and entities

A repository of fraudulent transactions involved entities and their modus operandi is a pre-requisite for sharing of information, for risk profiling of fraudulent entities, for developing fraud heat map across the country, for industry level reports and collective action etc. As discussed in Section I, the repository should include 3 type of cases - suspect cases, confirmed frauds and unconfirmed frauds. Since confirmed frauds are presently quite less in proportion due to weak investigation capacities, lack of evidence etc., inclusion of all 3 categories shall help in giving an overall picture.

It is to be clarified that the Repository primarily deals with 'external fraud', internal fraud which involves internal executives/members of an organization is an internal matter for the organization, best dealt in accordance with organization's own governance guidelines and provisions. Only where internal party is found colluding with another external party to fraud, the same should be reported to repository.

2.1. General Insurance Council Fraud Risk Management Portal and repository framework for National Health Authority

The General Insurance industry has been plagued with frauds both on policy & claims side for a long time and the GI Council has been working with insurers to help mitigate frauds in the industry. Towards this, the Council has worked with insurers for sharing data and has created a fraud risk

mitigation portal (FMRP). The aim of the portal is to work collectively in identifying individuals or entities who have been involved or suspected in defrauding the insurers. The insurers share this list with the Council as and when they identify and investigate such possible frauds and this list is accessible by all insurers.

It helps every insurer to be wary of transacting with such parties. In the long run, such a list would also help in shaming entities involved in proven frauds, thereby acting as a deterrent to other possible fraudsters. Presently the portal has a set of essential data points which are utilized for reporting suspected or proven cases of fraud. The GI Council shared with the Sub-group the set of data points captured by it in the Fraud Risk Management Portal.

Given that the PMJAY would scale-up significantly in coming few years, it is the right time to also create a repository of fraud under PMJAY. The key distinguishing feature of any platform to be considered for incorporation by NHA would be its ability to scale and effectively integrate with the PM-JAY ecosystem as well as how promptly it adapts to the changing needs of the stake-holders in the system now as well as with the evolution of the scheme in the days to come. This platform should enable easy reporting, capture, standardization and sharing of data.

Also given the difference in nature, scale, modus operandi etc. of frauds under private paid health insurance and that under PMJAY/Govt. schemes, it best suits the purpose for two repositories to be maintained separately. GI Council repository should be mandatory for reporting by insurance companies on fortnightly basis. NHA's repository should be mandatory for fortnightly reporting of frauds under PMJAY and other Govt schemes for single view of fraud under Govt schemes. Both repositories shall have common data points for easy sharing of relevant data across the repositories so that a collective thrust can be possible to mitigate frauds.

In due course – 1 year hence, there should be system level integration for sharing of data through APIs directly. The participating stakeholders working under IRDAI and NHA should have secure access to the repository data and should be able to draw reports, check details of specific entity etc.

2.2. Depth of data in the repository

While the depth and width of data elements in any repository help in more advanced analytics, the starting purpose of this repository is to create a compilation of all frauds under health insurance, starting with suspect transactions committed by different entities, taking the same to logical conclusion up till closure action. It would help various stake-holders while engaging with such

entities and in some cases to help in taking collective action against such entities. While the data structure and schema are discussed in the context of PMJAY, the same shall apply to reporting of frauds by other Govt schemes also as and when added to the Repository.

Under PMJAY, the data is structured broadly as under:

a) Beneficiary Identification System – beneficiary details, unique id, demographics
b) Transaction management system – patient details, case number, procedure carried out, amount blocked etc.
c) Hospital Empanelment Management system – details about empanelled hospitals, hospital unique id, the specialties available, infrastructure etc.
d) Package masters – List of all procedure packages with codes and specialty details

It is always possible to go back to any of these records for greater detail while maintaining the fraud reporting to the bare essentials. The idea is also to develop a repository that would facilitate the exchange of information between FRMP and NHA by utilizing the common fields thereby rendering a seamless mechanism of fraud reporting.

2.3. Convergence of the schemas and Repository Details

The schema is mainly divided into following sections (refer to Annexure 5) –

a) Patient Details
b) Fraudulent Entities
c) Suspicion Indicators
d) Investigation/Detection/and Action
e) Other Details

Details of each are mentioned as below -

a) Patient Details:

In any fraud reporting there is a basic transaction that triggers the investigation / suspicion. In health schemes this is linked to the claim made by a patient. This section captures the details of the patient in case of PMJAY or the insured in FRMP's parlance. Some of the key fields in this section are as follows:

i. **Card Number:** It is a unique identification card number allotted during the enrolment process.
ii. **Data Type: String**

iii. **Corresponding FRMP Field:** Policy Number

iv. **Patient ID Type**

v. **Description:** This is essentially an identification proof of the patient, a unique Govt. recognized ID like PAN, Voter ID, Aadhar Ration Card. We will get this data from BIS, where enrolment is done and card number is generated.

vi. **Data Type:** Drop Down with values – PAN, Aadhar Card, Voter ID, Ration Card, Driving License, Birth Certificate and Others.

vii. **Patient Address -** The will be address of the patient, which will be captured in more detailed level to capture city, district, block, state code and pin code which is presently prevalent in Beneficiary Identification System prevalent as per PMJAY guidelines.

viii. **Data Type:** String

In this Patient Details section, it is recommended to capture other details of the patient, which include Patient Family ID, Patient Name, Patient Age, Patient Gender, Patient ID Number. These will be helpful in referring back to the transactional data for greater details at any stage.

b) Fraudulent Entities:

This section comprises of the information about the suspect entities which are involved in committing the fraud that is being reported upon. Some of the key fields in this section are as follows -

i. **Entity Name:** This is the name of the entity which is involved in the underlying fraud.
   - **Data Type:** String
   - **Corresponding FRMP Field:** Individual Name /Company
     - **Entity ID :** ID Number of the entity involved in the fraud
     - **Data Type:** String

ii. **Entity ID DocType:** This field will capture the Government recognized ID proof of that entity
   - **Data Type:** Drop Down list consisting of PAN (Individual or company), Aadhar Card, Voter ID, Ration card, Driving license, Birth certificate, Passport, Registration number/CIN for corporations, GST number and others
   - **Corresponding FRMP Field:** ID Type

iii. **Fraudster (Suspect Entity) Type:** This field has been included to identify if the entity involved in the fraud is an individual or an organization
   - **Data Type:** Drop Down list consisting of Individual, Organization and others
   - **Corresponding FRMP Field:** Fraudster type – Individual/Organization

iv. **Fraudster (Suspect Entity) Category:** One of most important aspects of fraud reporting is to determine the level at which it is happening. There are several instances where there are entities who appear to be involved in silos but are actually colluding at different levels. This field tries to depict the possible categories of fraudsters who may be involved individually or collectively.

- **Data Type:** Drop Down list consisting of Provider, Beneficiary, Internal Insurer member, Policyholder, Intermediary, Payer fraud and Others
- **Corresponding FRMP Field:** Fraudster category (Fraudster category (Doctor/ Hospital/ Employee etc.)

v. **Fraudster Sub Category:** Based on the selection of Fraudster Category field, it will have the further bifurcation to enter sub-categories so as to provide further insights regarding the fraud category.

- **Data Type:** Drop Down list. The drop-down list will be dynamically updated based on the Fraudster Category field. If the Fraudster Category is selected as say Provider; then only the following drop-down list of sub-categories would come up. This will be similarly applicable to other fields.

For 'Provider' -

- Hospital
- Medical Practitioner/Treating doctor
- Diagnostic Centre
- Pharmacy
- PMAM
- Others

For 'Internal member' Fraud -

- Board Member / Senior Management
- Mid-Management Member
- Another employee

For 'Beneficiary' -

- Patient admitted in hospital
- Individual impersonating as beneficiary

For 'Intermediary' -

- Insurance Agent

- Corporate Agent
- CSC/VLE
- Others

For 'Payer Fraud' –

- Insurance Company
- State Health Agency
- TPA
- Implementing Support Agency
- IT provider
- Others

vi. **Fraud Classification:** This field would aid in earmarking the frauds into specific buckets so that it will provide an avenue to drill down further to capture the accurate details

- **Data Type:** Drop Down list consisting of Clinical fraud, Impersonation fraud, Counterfeiting, Misappropriation, Concealment, Cheating, Forgery, Falsification, Breach of Contract, Criminal breach of Trust and others.

vii. **Fraud Sub Classification:** This field would aid in providing a sub-classification of fraud.

- **Data Type:** Drop Down list consisting of unbundling, upcoding, phantom patients, billing for services not provided, kickbacks, off label marketing of pharmaceuticals, physician self-referrals, accepting bribes, prescription fraud, doctor switching, identity switch, not providing all services as charged/early discharge, non-licensed hospitals, non-registered doctors, wrongful cover and others.
- The drop-down list will not be dynamically populated based on the 'Fraud Classification' field selection unlike the Fraudster Sub Category field; but will always depict the same set of values so that the user can select the appropriate one which would be in line with the value selected in Fraud Classification field.

It is also recommended to capture the entity contact details and address, including latitude and longitude of the location as well as the details of the Director of the hospital / entity. The rationale of doing this is to prevent the same fraudsters from starting another operation under a different name either at the same or different location.

c) Suspicion Indicator Details

This section enlists the fields which provide insights on the underlying basis on which the fraud is identified.

i. **Case Number:** Case number which is reported in the fraud
   - **Data Type:** String
   - **Corresponding FRMP Field:** Claim Number

ii. **Fraud Index:** To categorize the fraud into confirmed/unconfirmed and suspicious. The field would provide information as to whether the underlying case has been reported as a confirmed fraud or a possible suspicion or unconfirmed.
   - **Data Type:** Drop down list comprising of values – Suspicious, Confirmed, Unconfirmed.
   - **Corresponding FRMP Field: Where suspected or proven case**

iii. **Modus Operandi:** A field depicting the underlying mechanism/method employed by the fraudsters to bring about the fraud.
   - **Data Type:** Free Text
   - **Corresponding FRMP Field:** Modus Operandi in Brief

iv. **Existing Legal Case Indicator:** To depict if any legal case is pending against the entity involved in the fraud.
   - **Data Type:** Drop down with values YES and NO
   - **Corresponding FRMP Field:** Any Legal Case Pending

v. **Name of Insurer/Trust:** This field depicts the Name of the insurer or trust. Here it doesn't imply that they are involved in fraud; but it is mainly to capture that information for further use
   - **Data Type: String**
   - **Corresponding FRMP Field:** Name of Insurer

Other fields captured relate to hospitals being marked in the watch list or not, fields related to claim history and claim count to uncover if the entity involved in the fraud/suspicion has any claims that were rejected previously.

d) Investigation/Detection/and Action:

This section will have details related to investigation and actions executed for the claim to identify and understand if the claim has been investigated and analyzed thoroughly. Some of the key fields in this section are as follows:

i. **Investigator Type:** This is mainly to cater to the type of investigator that will be assigned to the investigator, which will have categories of internal, external, including industry collaboration.

   Data Type: Dropdown with values - Internal Investigator, External Investigator, Internal and External investigator, Industry Collaboration and Others.

ii. **Investigation Type:** Investigation Type will capture the type of investigation performed to understand the claims reported.

   Data Type: Dropdown with values - On-field investigation, Investigation via call center, Desk audit and Others.

iii. **Action since confirmed:** This field will capture the action that is taken against the entity which has committed the fraud once the fraud is confirmed.

   Data Type: Dropdown with values - De-empanelled, Intermediary barred, Claim denied, Money recovered, FIR lodged, Reported to MCI/State Medical Establishment Act, Included in Name & Shame, Industry blacklisted, Hospital registration cancelled, Others.

iv. **Date of Action:** This field will capture the date when action is taken against the entity which has committed the fraud once the fraud is confirmed.

   Data Type: Date Format.

v. **Time Period of Action:** This field will capture the time period for which the Action is valid- Suspension/ De-empanelment/ Blacklisting in MCI may happen for a specified period.

   Data Type: Numeric in Months.

vi. **Amount recovered:** This field will capture the amount that was recovered from the entity involved in fraud as a part of the action

   Data Type: Dropdown with values - Claim amount Rs.____, Penalty Amount Rs. _____, Others Rs._____.

There are other fields which will help to analyze the fraud more efficiently and effectively which includes Investigator Name and important dates like Suspicion Reported Date, Fraud Confirmed Date.

In addition to the above sections, it is proposed to capture details related to Hospital Type, ROHINI ID, fields related to preauthorization and claims, admission and discharge dates, procedure and diagnosis details, treating doctor details etc. These fields are prevalent in the PMJAY schema and the idea is to utilize these fields and map it to the 'Claim Details' and the 'Case Details' fields prevalent in FRMP.

2.4. FRMP enhancement

The FRMP is a good beginning and has helped in building a culture of sharing data on frauds. There is a need to enhance width of information capture to enable a better tracking across other insurers / stakeholders about similar incidents. This would also help in greater sharing & collaboration with the PMJAY/Govt schemes eco-system.

2.5. Exchange of fields between FRMP and NHA repository

The sub-group has tried to identify the common fields between the schemas and have proposed new fields essential for fraud reporting, some of which are prevalent in FRMP schema. However, for the purpose of cross stake-holder (NHA & GI Council) sharing, it is recommended to share essential fields that help in a collaborative effort of preventing frauds, in "naming & shaming" and help in creating an overview of prevalence of fraud across India, fraudsters warranting collective action etc. The Patient details (Insured details) or the detailed case details are not recommended unless patient is proven to be involved in the case. Only the details pertaining to the fraud and entity which is allegedly involved in committing the fraud is to be reported, the suspicion indicator and the investigation details are marked for sharing.

2.6. Implementation

Once the above framework is approved for adoption in principle, the Sub-group shall work for development of both the repositories as well as mechanisms for sharing of data, MIS and reports on regular basis.

Both the schema will need to be evolved further to ensure the following:

a) Standardizing the nomenclature and codification across the industry/PMJAY eco system
b) Aid in manoeuvring of the fields across different IT systems
c) Broad-base the list of drop-down values, particularly in fraud type to ensure precise & comprehensive list of frauds

The details of all the fields in the schema along with the correlation with the FRMP fields has been described in **Annexure 5.**

It is also recommended that once Repositories are established, the sub-group should engage in detailed analytics exercise with help from IIB and publish industry level reports. If in future IIB sets up a repository to enable information sharing among insurers it should be compatible and aligned with this repository. Specialized advanced analytics, predictive models can also be carried out on request from a payer on paid basis.

3. Standards for field verification and investigation

An important aspect of anti-fraud measures relates to field verification and investigation of suspect or triggered cases. In the absence of good techniques and trained manpower for investigations, the success rate of confirmed fraud remains quite low. Presently there are no standards which are adhered across industry for collection of relevant information and vital documentary evidence. The persons involved in field verification learn mostly on the job, there being no standard training or certification for them. The talent pool of trained field verifiers simply does not exist.

Thus, there is urgent need to develop standards for field verification and investigation which should also form the basis of certification training of field verifiers. It is to be noted that the standard format here relates primarily to frauds committed by healthcare providers and not for other category of frauds. Also, the requirements of relevant data and documents differ in certain key aspects for private paid insurance and for PMJAY/Govt schemes.

The sub-group studied both the formats - used by different players in insurance industry presently and that developed by NHA for PMJAY field verification/investigation. From this a draft checklist for field investigation has been drawn. The checklist is based on points of verification which are:

- common to both the PMJAY/Govt schemes and private insurance,
- specific to PMJAY/Government schemes and
- specific to private paid insurance.

The investigation format is divided into three sections, namely - Member, Provider and Other Checks. In order to derive most effective results, it is advisable that investigators are provided details of specific triggers to focus on for carrying out appropriate investigation and collecting all relevant information/documentary evidence. The list of checks mentioned in the format is comprehensive for identifying various types of Fraud and Abuse. These are minimum checks

required to establish Fraud/Abuse. However, an investigator may look into additional information depending on the triggers and discovery during investigation.

It is advisable that the investigators are trained to look into appropriate information and draw conclusions in line with the triggers shared for investigation. For arriving at a conclusion of "Abuse" it is recommended that the findings from investigation are reviewed by Medical team of the payer organization.

3.1. Checks related to Member

Member section of investigation covers identification of member and collection of valid id proof. The aim is to identify the patient/member as the actual intended beneficiary of either Govt. Scheme or policy holder of private insurance. The questions are related to member's ailment, awareness around treatment, history of any ailment of family members, treatment details to identify fraud or abuse. Similarly, there are questions to gauge member's awareness around PMJAY to further identify instances of fraud by providers including those perpetrated without knowledge of beneficiary.

3.2. Checks related to Healthcare Provider and Claim/Transaction

Provider part of investigation covers identification of provider and collection of details related to treatment of the member/beneficiary. Investigator should perform checks related to registration details of patient's treatment, surgery & diagnostic tests performed, Internal case papers, hospital infrastructure etc. Information so collected should be matched with the treatment provided to note if treatment is provided is in line with the ailment, if infrastructure is commensurate with the treatment provided etc. These questions will help the investigator or the Claims processing Doctor in concluding presence of fraud or abuse.

3.3. Other Checks

These are more relevant in case of retail insurance or non-Government sponsored schemes. These questions or checks are intended to link findings from investigation such as employer check, neighborhood check.

Standard format is attached as Annexure 6

3.4. Implementation of standard investigation format – Technology platform

The standard format is an indicative list/guideline for minimum information that should be collected for proving fraud and abuse. A payer may desire additional information/documents or specific cases

may also require deeper probing. Once the standard format is accepted in principle, the sub-group would be required to work on synchronizing the check list with both Repositories and IIB.

Along with standard format, the technology platform also needs to be efficient, flexible and scalable. These checks can be built in an application with facility to capture maximum findings in Binary mode to reduce subjectivity in investigation considering the field investigator may not be a Medical Doctor. Further such form of data collection would help in building data repository facilitating deeper analytics. The application should enable capture and upload of evidences to match findings with available evidences. Such applications would help real time tracking of investigation, faster sharing of information with the offsite review teams and lend credibility to information so collected in view of geo location tagging.

NHA is planning to use a Real Time GPS enabled Field Investigation Mobile App for field investigation and medical audit and is in the process of customizing for capturing of necessary data, uploading of documents and integration of the same with end to end workflow. It allows multiple stakeholders – payer organization team and field investigators to interact on real time basis for allocation of cases, submission of report etc. There are other similar Mobile Apps available in the market for use, including few developed by in-house teams of insurance companies. The key is to use technology which is scalable and can be easily integrated with payer's core claims processing system.

3.5. Capacity Building

Along with standard format and technology to implement the same, it is equally critical to have trained talent pool to carry out effective field investigation job. A standard certification program shall help build this capacity. Usually the field investigators are neither from insurance industry or from medical field, thus the certification program should cover basic aspects of both along with deeper knowledge on investigation techniques.

a) At the minimum, an investigator should:
   i. be a graduate degree holder
   ii. have working knowledge of English and computer operation/ mobile app operation
   iii. good knowledge of regional language both written and spoken
   iv. not have conflict of interest (not be associated with alleged fraudster in any manner)

b) Course curriculum for investigator training program should essentially include:

i. Basics of health insurance, Govt schemes, key stakeholders, their respective roles
ii. Pre-authorization and claim process
iii. Basic processes in hospital for in-patient care, record keeping, billing practices
iv. Different types of frauds and abuse in health insurance
v. Verification and Investigation process
vi. Check list for verification at hospital, beneficiary/policy holder verification (in hospital/after discharge)
vii. Collection of documentary evidence specific to fraud trigger/case
viii. Communication and reporting skills
ix. Code of conduct

In addition to above standard content, depending on payer profile, the training course could include specific module e.g. PMJAY Anti-fraud Guidelines and procedure package familiarity for PMJAY or insurance company products, fraud management protocols for private paid insurance etc. For delivery of training course, it is preferable to have on-line digital learning portal/platform with/without class room-based training so that course can reach all districts and towns and help build talent pool where it is required. Training videos should be available in both Hindi and English. At least two-three organizations, expressing keenness to develop and deliver the course can be empaneled by IRDAI and NHA for delivery of training program.

It is recommended that once pilot for the training program is conducted by couple of training institutions, IRDAI and NHA should consider making certification course mandatory for any person – whether working individually as investigator or as an employee of an investigation agency and carry a unique registration number/Certified ID from IRDAI or NHA. If the investigation is carried out by an agency, it should have a registration number and its employees should mandatorily undergo certification training. In case of investigation by in-house team of insurance company, TPA or SHA, such payer organization shall ensure training by internal mechanism equivalent to standard training recommended above. An investigator visiting a hospital or beneficiary, or policy holder should be required to produce Certified ID, shall help in maintaining professional conduct and acceptance by hospitals.

This would ensure standardization of field investigation and capacity building ongoing basis as insurance penetration would expand and require more cases to be investigated. Different payers can

access/rely on investigation report of a registered investigator. In case of detection of a fraud ring/racket, affected payers may join hands and carry out collective investigation. The standardization can further be extended to the field of medical audits in next phase.

4. Name and Shame guidelines

4.1. Definition of 'Name and Shame'

"A system for public dissemination of information about an entity/person/organization involved in committing fraud under a health protection scheme of the Government or under an insurance program/policy."

Naming and shaming of fraud perpetrators in public domain/media is one of the mitigation strategies to deter health insurance fraudsters like hospitals and healthcare providers, intermediaries, policy holders etc. from committing malpractices. However, till date, the health insurance sector has not clearly defined the policies or guidelines around naming and shaming practices. The purpose of this Section to explore the existing naming and shaming practices in other industry - banking and develop guidelines for discussion and deliberation among the health insurance stakeholders in India.

4.2. Objective of 'Name and Shame'

The primary purposes of 'Naming and Shaming' are as follows:

a) To work as a punitive action against fraud perpetrators in health insurance sector, specifically healthcare providers/empanelled hospitals
b) To act as a deterrent for other healthcare providers from committing or perpetrating fraud and abuse or indulging in malpractices
c) To make the beneficiaries/policy holders/public and other payers/insurers aware of the hospitals involved in malpractices

The following aspects need to be considered to decide on taking the misconduct / malpractice by perpetrators, particularly hospitals, into the public domain:

- Seriousness of the misconduct/fraud/abuse
- Whether the misconduct was intentional
- Whether there were previous warnings, or a pattern of malpractices/abuses observed
- Whether the hospital tried to hide or mislead the SHA/Insurance Company or TPA
- Whether hospital extended co-operation in the audit and investigation

- Whether it merits collective action by other payers

While the focus under this section is on healthcare providers, insurance industry would benefit by developing the guidelines for intermediaries, rogue policyholders. The same may be taken up at later stage. However, presently capturing of the same in Repository shall give industry players an opportunity to develop a common view and knowledge of such entities and take action accordingly.

4.3. Key Considerations for drafting Name and Shame Guidelines

The most common notion of naming and shaming practices is to publicize the name of fraud perpetrators through various media channels including print, electronic and social media, among others. In case of health insurance sector, it needs to be ascertained if it would be prudent to publicize the names of fraud perpetrators in print and electronic media. That can act as a deterrent for future miscreants and also spread awareness in beneficiary and stakeholder community about the seriousness of this issue. However, in the absence of explicitly laid out laws and policies for naming and shaming, it has created an area of ambiguity around such practices, leaving it open to legal and judicial interpretation.

Naming and shaming in media can be legally questionable due to the following reasons:

- Naming and shaming is in conflict with Right to Privacy, which is a part of Right to Life guaranteed under Article 21 of the Constitution of India.
- Right to Privacy is also mentioned explicitly in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- Under International law also, the right to privacy has been protected in a number of conventions such as the Universal Declaration of Human Rights, 1948.

While there are examples to the contrary where public naming and shaming in print media has been upheld by the judicial courts in the banking sector, the overall ambiguity in these cases indicates naming and shaming practice through media campaigns is presently an uncertain strategy.

4.4. Recommendations on Name and Shame

The below mentioned recommendations – Phase 1 are made in present context for making a small beginning at different – incremental levels.

a) At Govt authority / agency / insurance firm / TPA level which has confirmed the fraudulent activity- Once the fraud / abuse / malpractice / misconduct is confirmed after investigation, due diligence and comprehensive medical audit, and the facts of the matter are verified and deemed to be correct, the authority / agency / insurance firm / TPA which has confirmed the said facts is recommended to initiate the following steps:

i. The Govt authority/SHA / agency / insurance firm / TPA would send warning or show cause notices to the hospitals found to be indulging in fraudulent activities, depending on the seriousness of the fraud

ii. The process of suspension and de-empanelment as per contract shall be followed. If the perpetrated malpractice is of serious nature and hospital is unable to satisfactorily explain/respond to show-cause notice or continues to indulge in malpractices, it would be removed from the list of network hospitals.

iii. A list of de-empaneled/blacklisted hospitals shall be mentioned on website of Govt. authority SHA/ agency / insurance firm / TPA website. The list should be prominently displayed and easily accessible on the website to ensure policy holder/beneficiary awareness and education.

iv. A separate list of hospitals served with warnings, show-cause notice or suspended temporarily shall also be mentioned on the website of Govt. authority/SHA/agency / insurance firm / TPA. The list should be prominently displayed and easily accessible on the website to ensure policy holder/beneficiary awareness and education.

v. A de-empanelled hospital may be allowed to re-apply for empanelment after a gap of minimum 6 months- 1 year if it submits proof of having mended its unethical ways and assures good conduct. However, if such hospital is again observed to be indulging in malpractices after re-empanelment and investigation confirms the malpractice, it should be permanently blacklisted by the payer.

vi. Concerned insurance firm / TPA shall inform IRDAI and share the list of hospitals blacklisted / de-empaneled / served warnings or show-cause notice on a monthly basis.

vii. In case of such hospitals being engaged with State Health Agency (SHA) for serving beneficiaries of AB PM-JAY or a Govt scheme, the SHA will share the list of such hospitals with the National Health Authority (NHA) on a monthly basis.

b) At Industry Level

i. It is recommended that all the stakeholders share the list of blacklisted / de-empaneled / hospitals served with show-cause notice or warnings on respective Repository.

ii. An “industry de-empanelled/blacklist” may be prepared by IRDAI on a monthly basis and displayed on its website. A similar “industry de-empanelled/ blacklist” will be prepared by NHA for hospitals empanelled with PM-JAY/Govt schemes.

iii. A “comprehensive industry de-empanelled/blacklist” of all hospitals blacklisted / de-empanelled should be shared in the form of a monthly circular with all insurance firms, TPA and other stakeholders involved in health insurance. It is recommended that all such stakeholders display the list on their website and update the same every month.

iv. The list should be prominently displayed and easily accessible on the website of all informed stakeholders to ensure policy holder/beneficiary awareness and education.

v. Press release should be issued by the IRDAI-NHA every month mentioning the list of hospitals de-empanelled and blacklisted.

c) Other initiatives

i. Policy holders and health workers shall be sensitized and informed about de-empaneled hospitals. They shall also be encouraged to bring forth complaints against hospitals or other entities engaging in malpractices/fraudulent acts.

ii. Industry/payer level use of bio-metrics for identification of policy holder at the time of availing benefits under a private paid insurance policy, not just under Govt. schemes can help prevent fraud.

iii. Whistle Blower mechanisms should be set up by every stakeholder/at individual organization level to facilitate confidential reporting of fraudulent actions, malpractices by hospitals, other entities.

iv. Hospital de-empanelled/blacklisted by one payer/organisation should be considered for blacklisting/de-empanelment by all payers so that it is impacted financially to a great extent. This shall act as strong deterrent for hospitals to indulge in malpractices.

v. De-empanelment/blacklisting at individual level of one insurer, one State or TPA does not have similar deterrence.

vi. Positive ratings of Payer community – State Health agencies and insurance companies along with policy holders and beneficiaries should introduce standards for rating hospital based on objective criteria relating to quality of care, overall facilitation, contractual compliance etc.

This would help the consumers of care to make informed choice and encourage competition amongst healthcare providers.

vii. Anti-fraud public messaging across industry/payers, recognition of organization/people with exemplary work in the area shall help build groundswell.

viii. As per the Code of Medical Ethical Regulations, 2002 of Medical Council of India (MCI), Chapter 8[2], if a medical practitioner is found guilty of professional misconduct, "the appropriate Medical Council may award such punishment as deemed necessary or may direct the removal altogether or for a specified period, from the register of the name of the delinquent registered practitioner. Deletion from the Register shall be widely publicized in local press as well as in the publications of different Medical Associations/ Societies/Bodies."

ix. In case of confirmed act of professional misconduct and violation of medical ethics (as per the clinical audit conducted), the appropriate Medical Council should be informed of the details of the case, the doctor and the hospital involved.

x. The Medical Council should take it up and take appropriate action as per the Code of Medical Ethics Regulation, 2002.

4.5. Legal framework for Effective Deterrence

All measures for anti-fraud shall remain incomplete and ineffective until backed by a strong enforceable legal framework e.g. how to recover money paid from a fraudulent hospital for false/manipulated claims without a long process of FIR and criminal prosecution or for effective 'name and shame' provisions which would deter fraudsters in big way, not just de-empanelment.

There is need for a specific anti-fraud law in health insurance with stringent provisions as prevalent in many countries, especially in countries where there is a large program like PMJAY. In the Philippines, the Philippine National Health Insurance Act contains overarching anti-fraud provisions supplemented with specific departmental (ministerial) orders. In Korea, it is included in the national health insurance law. In the United States, Center for Medicaid Services issues guidelines and training materials on anti-fraud, and fraud is clearly defined in five federal anti-fraud laws - False Claims Act, Anti-Kickback Statute, Physician Self-Referral Law, Criminal Healthcare Fraud, and Social Security Act.

[2] Code of Medical Ethics Regulation, 2002 (AMENDED UPTO 8th OCTOBER 2016), (Published in Part III, Section 4 of the Gazette of India, dated 6th April,2002); Medical Council of India Notification; https://www.mciindia.org/CMS/rules-regulations/code-of-medical-ethics-regulations-2002

In India, a strong law – National Health Insurance Anti-Fraud Act is required to effectively deal with whole gamut of activities for preventing, detecting and deterring fraud which would benefit entire eco-system including private paid health insurance. The law should provide for setting up of special anti-fraud task force to carry out punitive action, recoveries, search and seizure etc.

For international examples of Name and Shame guidelines refer to **Annexure 7.**

V. Recommendations and further collaboration

Joint collective measures by all payers shall have great impact on fraudulent practices of providers, which are the major players for fraud. It is recommended that all payers under the aegis of IRDAI, PMJAY and other Govt programs should work together and beginning can be made with following recommendations:

a) The definition of fraud and abuse should be standardized as per Report across eco system of health insurance/assurance schemes. Confirmation of a suspect transaction/event as 'fraud or abuse' should be done by concerned Payer after due-diligence and investigation.

b) All contracts signed by a Payer - with policy holder, empaneled hospital, intermediary, employee etc. should mandatorily incorporate standard definition of fraud and standard clauses as listed in the Report to enumerate the repercussions of committing fraud, range of punitive actions that may ensue.

c) Repository of fraudulent transactions, modus operandi and entities involved should be maintained at General Insurance Council (GI Council) level for insurance industry and at NHA level for PMJAY and all other Govt schemes. It should also include action taken by Payer.

d) Every Payer should be mandated by its governing authority i.e. IRDAI and NHA, to report both - suspect and confirmed frauds to respective Repository on fortnightly basis. In due course the data sharing should be done through APIs directly.

e) Both Repositories should have common minimum data points as suggested in the Report for data sharing, drawing of MIS, reports etc. and to develop 360* view of fraudulent parties, risk profiling, analysis of types of fraud and fraud Heat map of India across spectrum of Payers.

f) Standards for field investigation should be adopted with minimum common data/information as per Report both for private paid health insurance and PMJAY/Govt schemes.

g) A common talent pool should be created for effective investigation and a Certification program as per Report should be developed for ensuring minimum standards. In due course Certification should be made a mandatory requirement by IRDAI and NHA.

h) Name and Shame guidelines is an area for further development. A conservative approach is presently suggested in the Report in the absence of legal provisions in the country.

i) A strong legal framework needs to be conceptualized which should culminate in enactment of National Health Insurance Anti-Fraud Act by the Government.

Further collaboration between IRDAI and NHA along with stakeholder participation is required for implementation of Report as regards above recommendations pertaining to the 4 key deliverables, for governance and review mechanisms and for covering rest of areas in the realm of prevention, detection and deterrence of fraud and for drafting legal framework.

ANNEXURES

Annexure 1: PM-JAY Anti-fraud Guidelines 2018

ANTI-FRAUD GUIDELINES

Ayushman Bharat – Pradhan Mantri Jan Arogya Yojana (PMJAY)

Section 1. Purpose and Scope

1.1 **Anti-Fraud Guidelines** for the Ayushman Bharat – Pradhan Mantri Jan Arogya Yojana (PMJAY) is aimed at assisting state governments in designing and managing a robust anti-fraud system in PMJAY.

1.2 The scope of Anti-Fraud Guidelines cover prevention, detection, and deterrence of different kinds of fraud that could occur in PMJAY at different stages of its implementation:

Fraud management approaches	Stages of implementation
Prevention	- Beneficiary identification and verification - Provider empanelment - Pre-authorisation
Detection	- Claims management - Monitoring - Audits
Deterrence	- Contract management - Enforcement of contractual provisions

1.3 The Anti-Fraud Guidelines sets out the mechanisms for fraud management and lays down the legal framework, institutional arrangements, and capacity that will be necessary for implementing effective anti-fraud efforts.

1.4 For the purpose of the Anti-Fraud Guidelines, State Health Agency or the SHA means and refers to the agency or a unit set up by the state government to administer PMJAY in a state, irrespective of whether such entity is registered as a Society or a Trust or is a cell/unit/division within the Health Department of the state government.

Section 2. Health Insurance Fraud under the PMJAY

2.1 Principles

2.1.1 Any form of fraud under PMJAY is a violation of patients' right to health and misuse of public resources.

2.1.2 PMJAY is governed based on a zero-tolerance approach to any kind of fraud and aims at developing an anti-fraud culture that permeates all aspects of the scheme's governance. The approach to anti-fraud efforts shall be based on five founding principles: *Transparency, Accountability, Responsibility, Independence,* and *Reasonability.*

Understanding the terms:

i. *Transparency* shall mean public disclosure in decision making and in disclosing information as necessary in relation to PMJAY fraud.
ii. *Accountability* shall mean clear functions, structures, systems, and accountability for services for effective management.
iii. *Responsibility* shall mean management's conformity or compliance with sound organizational principles for PMJAY anti-fraud efforts.
iv. *Independence* shall mean a condition where the SHA is managed professionally without conflict of interest and under no compulsion or pressure from any party.
v. *Reasonability* shall mean fair and equal treatment to fulfil stakeholders' rights arising from agreements in PMJAY anti-fraud efforts.

2.2 Definition of fraud under PMJAY:

2.2.1 Fraud under the PMJAY shall mean and include *any* ***intentional deception, manipulation of facts and / or documents or misrepresentation made by a person or organization with the knowledge that the deception could result in unauthorized financial or other benefit to herself/himself or some other person or organisation. It includes any act that may constitute fraud under any applicable law in India.***

2.2.2 In addition to the above, any act (indicative list below) that is recognised by different provisions of the Indian Penal Code as *fraud* shall be deemed to be *fraud* under the PMJAY:

a. Impersonation
b. Counterfeiting
c. Misappropriation
d. Criminal breach of trust
e. Cheating
f. Forgery
g. Falsification
h. Concealment

Indian Contract Act 1972, Section 17:

"Fraud" means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto of his agent, or to induce him to enter into the contract:

1. the suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
2. the active concealment of a fact by one having knowledge or belief of the fact;
3. a promise made without any intention of performing it;
4. any other act fitted to deceive;
5. any such act or omission as the law specially declares to be fraudulent.

2.2.3 Human errors and waste are not included in the definition of fraud[1].

[1] **'Errors'** are un-intention mistakes during the process of healthcare delivery (like prescribing wrong medications to a patient). **'Waste'** refers to unintentional inadvertent use of resources (prescribing high cost medicines when generic versions are available). **'Abuse'** refers to those provider practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost to the PMJAY, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. It also includes beneficiary practices that result in unnecessary cost to the PMJAY. Whereas **fraud** is wilful and deliberate, involves financial gain, is done under false pretence and is illegal, **abuse** generally fails to meet one or more of these criteria. The main purpose of both fraud and abuse is financial and non-financial gain. Few examples of common health insurance abuse would be - excessive diagnostic tests, extended length of stay and conversion of day procedure to overnight admission.

2.3 Types of fraud under PMJAY and who may conduct fraud

Fraud under PMJAY may be conducted by either a beneficiary, a payer or a provider. Each type of fraud is described in the table below and illustrative examples for each type of fraud are listed in Annex 1.

Fraud type	Description
Beneficiary fraud	Fraud conducted by an eligible beneficiary of PMJAY or an individual impersonating as a beneficiary.
Payer fraud	Fraud conducted by a staff or consultant of NHA or SHA or personnel employed by any of the agencies contracted by the NHA or the SHA directly or indirectly involved with PMJAY. This could include but is not limited to Insurance Companies, Third Party Administrators, Implementation Support Agencies, IT solutions provider, and management, monitoring or audit agencies.
Provider fraud	Fraud conducted by any private or public health service provider empanelled for providing services under PMJAY.

Section 3. Responsibilities of National and State Health Agencies

3.1 Responsibilities of the National Health Agency

3.1.1 **Develop anti-fraud framework, guidelines and policies:** The NHA shall be responsible for developing national anti-fraud framework, policies, tools and guidelines to design and streamline anti-fraud efforts under the PMJAY. This responsibility shall include, among others:

a. Developing anti-fraud framework and guidelines which include this document and any other amendments or new guidelines that the NHA may issue from time to time;
b. Developing guidelines and standard operating procedures for different aspects of PMJAY such as beneficiary identification, provider empanelment, claims processing and management, monitoring and verification and audits.

3.1.2 **Provide broad oversight:** The NHA shall be responsible for providing broad oversight of PMJAY and for developing and implementing effective oversight plans to ensure that resources under PMJAY are used only for legitimate purposes. As part of this responsibility, the NHA shall:

a. Ensure that resources from all stakeholders are used as efficiently as possible to prevent and detect fraud and abuse;
b. Ensure that States have effective programme integrity systems in place, including the collection and validation of sufficient service delivery data to assess utilization and quality of care;
c. Develop effective communication framework for anti-fraud public messaging campaigns;
d. As required review current laws and regulations and develop legislative proposals to encourage appropriate statutes to support effective control of fraudulent activities;
e. Provide whistle blower mechanism for confidential reporting of fraud.

3.1.3 **Design IT infrastructure and protocols for advanced data analytics for fraud detection:** Specific tasks shall include but not be limited to:

a. Developing IT system design;
b. Integrating comprehensive list of fraud triggers into the IT system design;
c. Develop data standards and guidelines for data consolidation, mining and advanced analytics using predictive modelling, machine-learning models, regression techniques and social network analysis. Over a period of time, the NHA may integrate artificial intelligence and machine learning algorithms into the IT system for state-of-art fraud detection platform.

3.1.4 **Provide technical assistance to states:** The NHA shall provide need-based technical assistance to States in strengthening their anti-fraud efforts which may include but not be limited to:

a. Developing robust model contracts with fraud management clauses, punitive action and claw-back provisions;
b. Institutionalising effective internal control methods;
c. Developing specifications for IT-platform for the states;
d. Advanced data mining and analytics support including analysing inter-state anomalies;
e. Training on fraud management and programme integrity issues and, developing certification courses for district vigilance officers, field investigators, claim auditors;
f. Promote best practices through knowledge sharing;
g. Innovative techniques and mechanisms to stay ahead of perpetrators;
h. Sharing the list of suspect/black listed empanelled hospitals.

3.2 Responsibilities of the State Health Agency

3.2.1 **Develop institutional structures:** The SHA shall be responsible for developing institutional structures and operationalising them as per the guidelines set forth in Section 4 of the *NHA Anti-Fraud Guidelines*. It is recommended that appropriate government orders be issued by the State Governments to lend legitimacy to the structures and ensure that they are empowered to optimally perform their functions.

3.2.2 **Adapt and approve state anti-fraud policies and guidelines:** The SHA shall be responsible for adapting, wherever required, and adopting the NHA Anti-Fraud Guidelines to the implementation needs of PMJAY in their respective states. During adaptation the states may exercise freedom to align the provisions of these guidelines to their state-specific anti-fraud guidelines and/or practices, if they are already in place, while ensuring that the principles and the intent of the NHA Anti-Fraud Guidelines are not diluted in any manner and standard data sets are not tampered with.

3.2.3 **Recruit, deploy, train and manage anti-fraud human resources:** The SHA shall undertake the following tasks to ensure adequate human resource and capacity for anti-fraud efforts within the state:

a. Develop anti-fraud human resource plan on the lines indicated in Section 4 of the NHA Anti-Fraud Guidelines and seek appropriate approvals;
b. Ensure recruitment of required personnel as per the indicative skills and competencies set forth in Section 4;
c. Ensure training of all staff on PMJAY and on the state Anti-Fraud Guidelines.

3.2.4 **Develop IT system**: The SHA shall develop a state-specific IT platform which will include but not be limited to:

a. Transaction management software including claims management software that allows for submission, verification and approvals of pre-authorisations and claims;
b. Inter-operability to handle portability claims;
c. Develop comprehensive list of fraud triggers (see Annex 2) and embed the same in IT system, at relevant stages from beneficiary identification to payment and feedback;
d. Analyse data for trends, utilization patterns, outlier cases at individual level or for organised rackets/fraud rings;
e. Share data with the NHA for support in advanced fraud analytics.

However, SHAs shall have the flexibility to use the NHA IT platform if they so desire.

3.2.5 **Conduct anti-fraud awareness:**

a. Design and implement strategies for beneficiary awareness on possible episodes of fraud under the PMJAY. Awareness may include understanding types of fraud, its impact on beneficiaries, preventing measures that the beneficiaries could take and whom to report.
b. Beneficiary awareness on fraud may use mass media and interpersonal communication at the point of service. The Pradhan Mantri Arogya Mitras at the point of service could provide the beneficiaries a list of potential provider fraud along with the contact details for reporting episodes of fraud.
c. Design and implement strategies for medical community and provider awareness on what constitutes fraud under PMJAY, anti-fraud efforts under the PMJAY and implications of provider fraud and unethical practices.

3.2.6 **Develop and implement mechanisms for preventing and detecting all kinds of fraud under PMJAY including but not limited to beneficiary fraud, empanelment related fraud and claims related fraud.**

a. Adapt and adopt the NHA Anti-Fraud Guidelines including all other the relevant guidelines issued and amended by the NHA from time to time.
b. Ensure compliance to the guidelines approved by the state.

3.2.7 **Data analytics**

a. Set up mechanisms for data analytics for fraud detection. It essential for each state to have at least basic rule-based and outlier-based analytics and a comprehensive list of fraud triggers embedded within the IT system.
b. For advanced fraud-analytics, SHAs may seek the support of NHA.

3.2.8 **Contract design, management and enforcement**: The SHA shall be responsible for developing and managing contracts and providing oversight of all contracts issued by it. The contracts developed by the SHA shall have a clear definition of fraud, description and illustration of fraudulent practices, incentives and disincentives for anti-fraud efforts and the enforcement mechanisms. Contract management shall include monitoring of all contractual provisions and reporting obligations. The SHA shall develop compliance management tools and capacity to ensure time detection of gaps and implement corrective actions.

Contracted agencies of the SHA, like the Insurance Companies and TPAs / ISAs, shall set up their own anti-fraud units, develop their own fraud management systems and processes and deploy required personnel as a part of their contractual obligation to the SHA. This does not substitute the fraud management efforts and oversight responsibility of the SHA and it is recommended that SHAs set up their own fraud management systems as per these Anti-Fraud Guidelines.

Section 4. Institutional Arrangements for Anti-Fraud Efforts

4.1 Dedicated Anti-Fraud Cell at the national level

4.1.1 **Mandate and functions**: The NHA shall constitute a dedicated Anti-fraud cell (National Anti-Fraud Cell) at the national level. The mandate of the National Anti-Fraud Cell shall be to:

a. Provide leadership stewardship to the national anti-fraud efforts under PMJAY;
b. Develop, review and update the national anti-fraud framework and guidelines based on emerging trends;
c. Provide mentoring support to states in setting up and institutionalising the in-state anti-fraud efforts;
d. Capacity building of states on anti-fraud measures under PMJAY;
e. Liaise with the national IT team / agency to ensure that the IT platform is periodically updated with fraud triggers based on review of trends;
f. Liaise with the monitoring unit of the NHA for triangulating fraud related data analytics with the overall service utilisation trends emerging under PMJAY;
g. Provide evidence-based insights to states on trends emerging from state-specific fraud data analytics;
h. Handle all fraud related complaints that the NHA may receive directly and liaise with the states from any complaints specific to states as per Anti- Fraud Guidelines and Grievance Redressal Guidelines of PMJAY;
i. Take *Suo moto* action based on prima facie evidence as deemed appropriate;
j. Establish whistle blower mechanism, public disclosure guidelines, and other deterrent measures.

4.1.2 **Location and structure of the National Anti-Fraud cell**: The National Anti-Fraud Cell should:

a. Be an independent unit in the NHA reporting directly to the CEO of the NHA;
b. Be headed by an officer not less than the rank of Director in the Ministry of Health and Family Welfare, Government of India, who shall have the designation of Executive Director (Anti-Fraud Cell). If possible, it is recommended that the National Anti-Fraud Cell head may be an expert with background in medical forensics.
c. Have three senior officials as General Manager / Deputy General Manager for each of the following three disciplines: Medical, Data Analytics and Legal & Vigilance.
d. Have at least 6 full time anti-fraud officers under the Anti-Fraud Cell Head responsible for the following category of states:

State Category	States included	No. of full time anti-fraud officers
HFS (NE) *8 states*	Arunachal Pradesh, Assam, Manipur, Meghalaya, Mizoram, Nagaland, Sikkim, Tripura	1
HFS (non-NE) *10 states*	Bihar, Chhattisgarh, Himachal Pradesh, Jammu Kashmir, Jharkhand, Madhya Pradesh, Odisha, Rajasthan, Uttar Pradesh, Uttarakhand	2
Non-HFS (large) *11 states*	Andhra Pradesh, Goa, Gujarat, Haryana, Karnataka, Kerala, Maharashtra, Punjab, Tamil Nadu, Telangana, West Bengal	2
Non-HFS (small & UTs) *7 states*	Andaman & Nicobar Islands, Chandigarh, Dadra & Nagar Haveli, Daman & Diu, Delhi, Lakshadweep & Pondicherry	1

e. Alternately, NHA may deploy Anti-Fraud Officers based on geographical cluster of states preferably with not more than 5 large states assigned to each officer.
f. The 6 Anti-Fraud Officers should be selected to offer complementary skills sets and competencies (for example, medicine, data analytics, clinical audit, field investigation, legal, etc.) while having distinct state responsibilities.
g. Anti-Fraud Officers responsibilities may include but not be limited to:
    i. Assessing fraud management capacity needs of assigned states;
    ii. Liaising with the Anti-Fraud Cells in the SHAs and provide mentoring support;
    iii. State-specific fraud-episode profiling and analysis with the support of the IT team;
    iv. Develop evidence-based state-specific recommendations for strengthening state-level anti-fraud efforts;
    v. Visit states as required;
    vi. Provide recommendations for course-correction in the PMJAY design based on anti-fraud data analytics.

Refer to Annex 3 for organogram of the Anti-Fraud Cell in the NHA and indicative terms of reference for various positions.

4.2 Dedicated Anti-Fraud Cell in states

4.2.1 **Mandate and functions**: The SHA shall constitute a dedicated Anti-Fraud cell at the state level. The mandate of the Anti-Fraud Cell shall be to:

a. Provide stewardship to the state level anti-fraud efforts under PMJAY;
b. Develop, review and update the state anti-fraud framework and guidelines based on emerging trends for service utilisation and monitoring data;
c. Ensure that the state Anti-Fraud Guidelines are consistent with the national Anti-Fraud Guidelines issued by the NHA from to time;
d. Capacity building of the state PMJAY team on anti-fraud measures under PMJAY including field verification and investigations;
e. Liaise with the IT team / agency to ensure that the IT platform is periodically updated with fraud triggers based on review of trends;
f. Liaise with the monitoring unit of the SHA for triangulating fraud related data analytics with the overall service utilisation trends emerging under PMJAY;
g. Provide evidence-based insights to the SHA on trends emerging from state-specific fraud data analytics;

h. Handle all fraud related complaints that the SHA may receive and liaise with other departments of the SHA, specially the monitoring and the audits departments;
i. Take *Suo moto* action based on prima facie evidence as deemed appropriate;
j. Undertake fraud investigations as required, prepare investigation reports that can stand legal scrutiny if needed, file First Information Reports with the police as needed, navigate the legal system, pursue recovery and all other tasks related fraud investigation and follow up actions, including if required notice to treating doctors, etc.
k. Incentivising internal team/outsourced agency involved in fraud management based on performance;
l. Publish data on utilization, claim rejection, suspension, dis-empanelment, etc.

4.2.2 **Location and structure of the anti-fraud cell**: The state Anti-Fraud Cell should:

a. Be an independent unit in the SHA reporting directly to the CEO of the SHA;
b. Be headed by an officer not less than the rank of Director in the Department of Health and Family Welfare of the state government, who reports directly to the CEO of the SHA. If possible, it is recommended that the state Anti-Fraud Cell head may be headed an expert with background in medical forensics.
c. Recommended staffing pattern for the Anti-Fraud Cell under the Insurance, Assurance, and mixed (both insurance and assurance) modes:

	Insurance Mode	Assurance and Mixed Mode
State level Anti-Fraud staff		
Head	1	1
Officers	1	1 for every 10 districts
District & facility level staff		
District Vigilance & Investigation Officers	1 in each district	1 in each district
Pradhan Mantri Arogya Mitras (PMAM)	Minimum 1 PMAM to be available 24&7 in each empanelled provider	Minimum 1 PMAM to be available 24&7 in each empanelled provider

d. To avoid possibilities of collusion, it is recommended that the District Vigilance & Investigation Officers be directly recruited by the SHA.
e. To ensure adequate capacity and skills, it is recommended that all anti-fraud staff be recruited from among ex-servicemen.
f. To avoid collusion, if possible, the SHA should try and rotate Pradhan Mantri Arogya Mitras every 3-6 months preferably within the same city / town.

Refer to Annex 3 for organogram of the Anti-Fraud Cell in the SHA and indicative terms of reference for various positions.

4.3 Core competencies in the Anti-Fraud Cells

The Anti-Fraud Cell should have the following minimum core competencies and skills:
a. Legal skills
b. Case investigation skills
c. Claims processing
d. Medical specialist
e. Medical audit

f. Medical forensics

4.4 Other committees at the state

4.4.1 Claims Review Committee (state level):

a. A Claims Review Committee (CRC) is recommended at the State level within the SHA.
b. Constitution of the CRC:
    i. The CRC may be headed by the Medical Management and Quality Manager of the SHA;
    ii. Other members may include a panel of experts from the insurance / TPA industry and medical specialists from apex government medical institutions and medical colleges.
c. Functions of the CRC:
    i. Review 100 percent claims that are rejected by the Insurer / TPA / ISA / SHA and appealed by the provider;
    ii. Randomly review / audit at least 2 percent of the pre-authorisations and 3 percent of the claims of each provider each quarter.

4.4.2 Mortality and Morbidity Review Committee (state level)

a. A Mortality and Morbidity Review Committee (MMRC) is recommended at the state level within the SHA.

b. Constitution of the MMRC:
    i. The MMRC may be headed by the Medical Management and Quality Manager of the SHA;
    ii. Other members may include medical specialists as required from apex government medical institutions and medical colleges.

c. Functions of the MMRC:
    i. The scope of MMRC review shall include assessment of line of treatment, review of medical and patient progress records, prescription practices and determine whether the treatment provided is in line with good clinical practices;
    ii. Review 100 percent of mortality claims;
    iii. Undertake fraud-trigger based review and audit of cases as recommended by the medical audit team or the claims processing team;
    iv. Review high value/complex surgical/uncommon procedure code claims.

4.5 Role of existing health department structures in strengthening anti-fraud oversight

4.5.1 It is important to integrate and institutionalise anti-fraud efforts within the state health department and health systems at the state and sub-state levels.

4.5.2 At the state level, each state may develop mechanisms for involving the Health Directorate in anti-fraud oversight.

4.5.3 A large number of states have administrative structures and set up at the regional / divisional level. Each divisional / regional unit is responsible for monitoring of health department operations in a cluster of districts. The feasibility of engaging these regional / divisional units in monitoring and anti-fraud oversight of PMJAY is recommended.

4.5.4 At the district level, existing governance and monitoring structures such as the District Health Societies or the Zilla Parishads (in states where the local self-government structures at the district level are strong), may be leveraged upon.

4.5.5 States that may have set up community-based monitoring mechanisms may consider leveraging upon such structures to involve local communities for reporting unethical / fraudulent practices / behaviour.

4.6 Operations and management of the anti-fraud cell at the state level

4.6.1 **Nodal responsibility**: The Head of the Anti-Fraud Cell shall be the nodal person responsible for all anti-fraud efforts within the state.

4.6.2 **Annual plan and budget**: The Anti-Fraud Cell shall develop an annual anti-fraud response plan which may include but not be limited to:

a. Statement detailing detecting fraud cases with like the agency / individual committing fraud, type of fraud, time taken for detecting and proving the fraud, update on action-taken reports filed and pending and relevant other details;
b. Typology of fraud detected in the last financial year and disaggregation of cases by types of fraud:
c. Any new strategies that may need to be adopted based on the analysis of last year's fraud data;
d. Additional capacity need, if any;
e. Budget (all activities related to anti-fraud efforts as per the plan to be budgeted).

The anti-fraud action plan and budget needs to be approved by the Executive Committee or the Governing Board of the SHA and funds should be made available to the SHA.

4.6.3 **Review of anti-fraud efforts**: Apart from review meetings as and when required, the Anti-Fraud Cell shall ensure at least a quarterly structured anti-fraud meeting with the SHA management team. Alternately, anti-fraud efforts review could feature as a part of the ongoing review meetings of the SHA. All discussions and decisions thereof should be minuted and the head of the Anti-Fraud Cell shall ensure follow-up actions as per decisions taken.

Section 5. Guidelines for Anti-Fraud Measures

5.1 Guidelines for fraud prevention

5.1.1 **Develop anti-fraud policies and guidelines**: Based on the national Anti-Fraud Guidelines, it is recommended that the states develop their own anti-fraud framework and policies/ guidelines for PMJAY to account for the implementation-specificities of their respective states. The Governing Body of the SHA should approve the state Anti-Fraud Guidelines prior to implementing the PMJAY. The SHA should ensure that all staff are trained on the approved state Anti-Fraud Guidelines.

5.1.2 **Develop referral protocols for benefits that are more prone to fraud and abuse**. Procedures or certain benefits under PMJAY that are more prone to fraud may be either reserved only for empanelled public providers or can be availed only on referral from a public provider. The SHA should issue appropriate orders to this effect.

5.1.3 **Ensure that all contracts signed by the SHA with any party (Insurer, ISA, TPA, provider, IT agency, etc.) have adequate anti-fraud provisions that are enforceable.** The SHA should ensure that all model contracts available on PMJAY website that are adapted by the states have a clear definition of abuse and fraud, what constitutes abuse and fraud and what are their consequences. Liabilities of different parties concerned should be clearly spelt out in the contract. The SHA should ensure that the contracts have adequate disincentives and penalties for abuse and fraud.

5.1.4 **Preventing empanelment fraud:** The SHA shall ensure strict compliance to the NHA guidelines for empanelment of providers. In addition, to further reduce empanelment related fraud, the SHA may publish hospital-wise empanelment assessment scores on PMJAY website of the state to allow any third party to report false capacity representation made by any provider. Annual assessment / audit of all empanelled providers by an independent agency with relevant experience is recommended to ensure compliance to the minimum empanelment criteria. Extra caution should be exercised during initial and follow up providers assessments especially in those states that have provisions of awarding assessment grades and have differential grade-based tariff.

5.1.5 **Beneficiary identification / verification:** The SHA shall ensure strict compliance to NHA guidelines for beneficiary verification. For beneficiary fraud prevention, the Anti-Fraud Cell shall track the conversion of beneficiary records from 'silver' to 'gold', which indicates that the beneficiary details are verified. When a beneficiary reports to an empanelled provider for treatment, the Arogya Mitra enters the beneficiary details on the Beneficiary Identification System of the transaction software. After the beneficiary verification is complete, the record is inserted into the system as a 'Silver' record, which gets converted to 'Golden Record' after further verification and approval by the designated authorities. For further details, refer to the NHA guidelines on 'Arogya Mitras' and 'Guidelines on Process of Beneficiary Identification' available on the NHA website.

5.1.6 **Pre-authorisation:** The SHA shall ensure strict compliance to NHA guidelines for pre-authorisation. In addition, to further strengthen the efforts to pre-authorisation fraud, the SHA shall:

a. Develop detailed pre-authorisation protocols and automate the process including mandatory submissions into the claims management software as an automated workflow process;
b. Ensure SMS updates to beneficiaries on pre-authorisation decision and amount blocked procedure proposed to be carried out etc in local language and another SMS at the time of discharge;
c. Ensure auto-cancellation of pre-authorisation approvals if services are not sought and records are not updated on the transaction platform by the provider within 30 days of issuing the pre-authorisation.

5.1.7 **More important for states going through the Assurance mode:** Financial risks to the state government on account of fraud is significantly higher in assurance mode than in the Insurance mode, where the Insurer bears the risk and the outgo of the state government is limited to the premium paid. Therefore, it is recommended that the SHA, especially for states implementing PMJAY though the Assurance mode (even the states following the Insurance route may adopt these practice), may set up a separate committee(s) of senior government

staff for high-value pre-authorisation requests for different threshold levels (states may set up their own thresholds for high value pre-authorisation requests).

5.2 Guidelines for fraud detection

5.2.1 Claims management

a. The SHA shall ensure strict compliance to NHA guidelines for claims management.
b. Claim data analysis for early detection of fraud shall be conducted fortnightly by the Anti-Fraud Cell.
c. Such claim data analysis shall be conducted through the following approaches:
    i. Identifying data anomalies trigger based and rule-based analysis;
    ii. Advanced algorithms for fraud detection, predictive / regression based and machine learning models and other advanced data analytics reports received by the SHA from the NHA or as requested by the SHA to the NHA, provided the SHA makes all claims data available to the NHA for analysis.

d. In conducting claim data analysis, the Anti-Fraud Cell may coordinate with the medical audit team of the SHA, claims processors and adjudicators in the TPA / ISA or the CRC or the MMRC (refer to Section 4.4) and other parties as necessary.

5.2.2 Fraud detection during routine monitoring and verification: The key to an effective anti-fraud and abuse programme is to gather information on provider performance. The Anti-Fraud Cell within the SHA should combine the following techniques to detect fraud:

a. Data analysis comparing providers on such indices as utilization, performance, outcomes, referrals, disenrollment, followed by focused reviews on areas of aberrancy;
b. Routine reviews on particular problem areas;
c. Routine validation of provider data;
d. Random reviews and beneficiary interviews;
e. Unannounced site visits; and
f. Use of feedback and quality improvement.

5.2.3 **Comparative analysis:** The Anti-Fraud Cell may elect to perform a comparison of empanelled providers within districts or state-wide. Individual patterns of providers may not be significantly unusual but the cumulative pattern within a provider may require further review. It is recommended that the SHA's data systems be used to identify benefit utilization patterns that may assist in the case development and in the review.

5.2.4 **Routine reviews on problem areas:** As part of its fraud and abuse strategy, the Anti-Fraud Cell may identify areas of a focus that will receive special attention during routine monitoring of provider activities. These areas should be identified through systematic risk assessment, and could include, but not be limited to, items such as:

a. ensuring that providers within networks are eligible to participate in PMJAY;
b. ensuring that beneficiaries claimed as enrolled are in fact enrolled;
c. ensuring that provider employees understand PMJAY guidelines, can define fraud, and know where, how, and when to report it.

5.2.5 **Random reviews and beneficiary interviews:** The SHA should plan for a minimum level of random reviews, in which a selected universe of beneficiaries are contacted for interviews. Medical records should also be reviewed to identify any possible errors or evidence of abuse and/or fraud. All such reviews shall be as per the guidelines issued by the NHA from time to time.

5.2.6 **Unannounced site visits:** SHA monitoring plans should include unannounced provider visits, particularly to those providers for which some significant concerns exist. During unannounced provider visits, reviewers can observe encounters, interview beneficiaries or employees, confirm the accuracy of facility-based information, and/or review records.

5.2.7 **Use of feedback and quality improvement:** The results of reviews (including feedback from local communities, health workers) and investigations should be used to improve PMJAY implementation systems. The goal is to prevent the same fraud and abuse from recurring. This use of feedback is integral to PMJAY quality improvement.

5.2.8 Recommended minimum sample for audits:

Audit Type	Sample for Insurer / TPA audit	Sample for SHA audit
Medical audit	5% of total cases hospitalised	2% direct audits + 2% of audits done by the Insurer / TPA /ISA
Death audit	100%	100%
Hospital audit	Each empanelled hospital at least twice each year	Each empanelled hospital at least twice a year
Beneficiary audit (during hospitalisation)	10% of total cases hospitalised	5% direct audits + 10% of audits done by the Insurer/TPA /ISA
Beneficiary audit (post discharge – through telephone)	10% of total cases hospitalised	5% direct audits + 10% of audits done by the Insurer/TPA /ISA
Beneficiary audit (post discharge – through home visit)	5% total cases hospitalised	2% direct audits + 2% of audits done by the Insurer /TPA /ISA
Pre-authorisation audit	10% of total pre-authorisations across disease specialties	2% of audits done by the Insurer / TPA /ISA for Insurance mode) 10% of audits done by the TPA /ISA (for Assurance mode)
Claims audit (approved claims)	10% of total claims	3% of audits done by the Insurer /TPA /ISA for Insurance mode) 10% of audits done by the TPA /ISA (for Assurance mode)
Claims audit (rejected claims)	-	100%

5.3 Guidelines for deterrence

5.3.1 Sound contracts, strong contract management, prompt action, speedy adjudication and strict enforcement of penalties and contractual provisions act as strong deterrence for fraud.

5.3.2 To enable the SHA to take firm actions against fraud including dis-empanelment and delisting of providers, it is recommended that a panel of providers be shortlisted and a waiting-list of to-be empanelled providers prepared.

5.3.3 However, in geographical locations with limited provider presence, the SHA may be constrained to dis-empanel or delist providers. In such situations, that SHA may consider more stringent penalties and firm disciplinary actions.

5.3.4 Public disclosure of providers who have engaged in fraudulent activities may act as a deterrent.

5.3.5 The SHA may demand the providers to take firm action including issuing warnings and show cause notices to treating doctors found indulging in unethical practices under the provisions of the Medical Council of India.

5.4 Monitoring effectiveness of anti-fraud measures

5.4.1 Periodic review of anti-fraud measures is required to improve the quality of the measures and to ensure that the anti-fraud efforts remain responsive and robust. A set of illustrative indicators for measuring the effectiveness of anti-fraud measures is provided in Annex 4. The SHA is at liberty to add more indicators as per its need.

5.4.2 The Anti-Fraud Cell may set up mechanisms of quarterly reporting against these indicators and recommend corrective measures to the SHA as required.

Section 6. Use of IT in Anti-Fraud Efforts

6.1 IT infrastructure for detecting fraud: The SHA should set up an IT infrastructure for seamless management of the PMJAY process that include:

a. beneficiary identification and verification module;
b. hospital transaction module;
c. pre-authorisation module;
d. claims processing module;
e. grievance redressal module;
f. hotline module.

6.2 Fraud triggers: The IT infrastructure should have a comprehensive fraud triggers based on which for automated alerts based on basic outlier analysis and rule-based analysis could be generated. A list of illustrative fraud triggers in provided in Annex 2. It is recommended that the Anti-Fraud Cell should constantly review the list of triggers in coordination with the Monitoring and Evaluation unit and the audit unit of the SHA and the IT platform be constantly updated with new triggers as needed.

6.3 **Data mining and analytics**: The IT infrastructure set up by the SHA is expected to have at least the basic fraud data analytics that allows for rule-based and outlier-based analysis. The NHA shall set up a centralised IT architecture for advanced analytics that may include predictive modelling, regression techniques and use of social network analysis. It is expected that the SHA shall allow NHA complete access to its transaction data for the NHA to provide fraud-analytics support to the SHA. Data analytics shall include retrospective and prospective analysis approaches. Whereas retrospective analysis will help identify patterns of fraudulent behaviour based on historical information, prospective analysis will analyse current data on a case-by-case basis to determine the legitimacy of claims.

6.4 **Automated tools to assist in fraud management**: The IT platform shall have automated security layers and tools to detect fraud. Security within data processing systems, segregation of responsibilities to prevent conflict of interest and ensure internal checks and balances, password and confidentiality policy are important to prevent fraud. This also includes development and use of a unique provider identification mechanism through which claims submitted electronically may be traced to their origin.

Section 7. Managing fraud complaints

7.1 Fraud under PMJAY may either be detected internally by the PMJAY staff lead by the Anti-Fraud Cell or be externally reported. Sources of information and mechanism of reporting are provided in the table below:

Internal detection sources	External reporting
- Audit reports (internal and external) - Monitoring reports - Filed visit reports - Routine validation of provider data - Random reviews and beneficiary interviews - Unannounced site visits - Use of feedback and quality improvement - Data analytics dashboard – including comparing providers on such indices as utilization, performance, outcomes, referrals, disenrollment, followed by focused reviews on areas of aberrancy	- From any individual or agency irrespective of whether they are engaged with or are beneficiaries of PMJAY or not - In writing through email / fax / letter to the SHA or the NHA or the grievance redressal cells that may be set up by the state government directly under the supervision of the Chief Minister - On PMJAY national or state helplines/call centre - On grievance redressal helplines, if any, set up under the Chief Minister's office

7.2 Subject to provisions under law, the SHA shall ensure that the identity of those filing grievances filed related to suspected fraud shall be kept confidential until the investigation is completed and it is ascertained that fraud has been committed.

7.3 On receipt of any complaint related to suspected fraud, the Anti-Fraud Cell shall promptly initiate action as follows:

a. Designate a nodal person to lead the enquiry and management of the case.
b. Within 48 hours, undertake preliminary examination to make a prima facie assessment. For a prima facie assessment, the Anti-Fraud Cell should analyse available data to create a hypothesis and test it against available facts to arrive at a reasonably certain prima facie conclusion that an act of fraud may have been conducted.
c. If there is prima facie evidence of fraud, the Anti-Fraud Cell shall take all measures required to initiate detailed investigation.
d. For detailed investigation, the Anti-Fraud Cell shall constitute an investigation team that will be headed by the concerned District Vigilance Officer. The head of the investigation team shall report to the Chief Vigilance Officer (CVO) of the SHA. Other members of the investigation team may include members of the medical audit team, monitoring and evaluation team, district level staff as the CVO of the SHA may deem appropriate. The CVO may, at her / his sole discretion, decide on the inclusion of staff from the ISA / TPA in the investigation team.
e. The investigation team shall undertake a thorough assessment which may include but not be limited to on-site enquiry, verification of original records, oral examination of concerned individuals, and submit a detailed investigation report to the CVO within 7 working days. The investigation report shall at the minimum include all details of the ooccurrence of fraud found; recommendations to prevent similar future reoccurrence; and recommendations to impose sanctions on fraud actors.
f. If the investigation report confirms fraud, the SHA shall, through appropriate levels within the SHA, issue a show-cause notice to the accused entity providing it with 3 days' time to respond to the allegations and present its defence.
g. Following the principles of Natural Justice, the Anti-Fraud Cell shall, within 2 weeks of receiving the response from the accused, communicate its final decision in the matter.
h. If the final decisions are related to suspension or dis-empanelment of an empanelled provider, the SHA shall abide by the detailed guidelines for disciplinary proceedings and dis-empanelment set forth in the NHA Guidelines on "Process for Empanelment of Hospitals" and the provisions of the provider contract.

Annex 1 Types of Fraud – Some examples

Beneficiary fraud:

a. Making a false statement of eligibility to access health services;
b. Knowingly allowing impersonation / identity theft in own name by another person to access health services;
c. Using their rights to access unnecessary services by falsifying their health conditions;
d. Giving gratifications / bribes to service providers for receiving benefits that are excluded/uncovered under PMJAY;
e. Engaging in a conspiracy with service providers to submit false claims;
f. Knowingly receiving prescribed medicines and/or medical devices for resale.

Payer fraud:

a. Engaging in a conspiracy with health facilities to falsify information with the aim of meeting empanelment criteria/becoming empanelled under the PMJAY;
b. Engaging in a conspiracy with beneficiaries and/or service providers to submit false claims for reimbursement;
c. Manipulating beneficiary list/covered members list;
d. Manipulating uncovered benefits into covered benefits;
e. Withholding legitimate claims payments to service providers to take personal advantage;
f. Not taking action against complaints of fraud received against provider(s).

Note: Reference to 'any of the agencies contracted by the NHA or the SHA directly or indirectly involved with PMJAY' in this para include but are not limited to Insurance Companies, Third Party Administrators, Implementation Support Agencies, IT solutions provider, management consultants / agencies, and monitoring and audit agencies.

Provider fraud:

a. Getting empanelled through manipulation of records or service/facilities etc.;
b. Manipulating / fudging claims for services covered under other state schemes and interventions and paid out of state budget;
c. Staff of public providers receiving some payment/commission/referral fees from private empanelled providers for referring beneficiaries;
d. Delays in scheduling treatment in anticipation of financial gain from beneficiaries or luring beneficiaries of preferential and early treatment in lieu of bribes;
e. Collecting unauthorized fees from beneficiaries;
f. Giving beneficiaries an inappropriate referral in order to gain a particular advantage;
g. Staff in empanelled public provider referring beneficiaries to private providers in exchange for financial considerations from the private providers;
h. Diagnosis upcoding (change of diagnosis code and/or procedure to a code of higher rate) and procedure code substitution;
i. Cloning of claims from other patients (duplication of claims from other patients' claims);
j. Phantom visit (claim for patients' false visit);

k. Phantom procedures (claim for procedures never performed);
l. Phantom billing (claim for services never provided);
m. Services unbundling or fragmentation (claim for two or more diagnoses and/or procedures that should be in one service package in the same episode or separate claims for a procedure that should be submitted in one service package in order to produce a larger amount of claims in one episode);
n. Duplicate/repeated billing (claim repeated for the same case);
o. Cancelled services (claim for services that are cancelled);
p. Measures of no medical value (claim for measures taken inconsistent with medical needs or indications);
q. Unnecessary treatment and/or medically inappropriate treatment;
r. Readmissions diagnoses and/or measures for one episode claimed for more than one time, as if for more than one episode;
s. Provision of counterfeit medicines;
t. Indulging or conniving to indulge in unethical practices not permissible under guidelines of Medical Council of India/State Medical Council for medical practitioners or Clinical Establishment Act or under any other law of land or established medical norms, whether leading to patient harm, future health endangerment of member or not;
u. Arogya Mitras colluding to refer patients to a competing empanelled provider.

Annex 2 Fraud Triggers

Claim History Triggers

1. Impersonation.
2. Mismatch of in house document with submitted documents.
3. Claims without signature of the beneficiary on pre-authorisation form.
4. Second claim in the same year for an acute medical illness/surgical.
5. Claims from multiple hospitals with same owner.
6. Claims from a hospital located far away from beneficiary's residence, pharmacy bills away from hospital/residence.
7. Claims for hospitalization at a hospital already identified on a "watch" list or black listed hospital.
8. Claims from members with no claim free years, i.e. regular claim history.
9. Same beneficiary claimed in multiple places at the same time.
10. Excessive utilization by a specific member belonging to the beneficiary Family Unit.
11. Deliberate blocking of higher-priced package rates to claim higher amounts.
12. Claims with incomplete/ poor medical history: complaints/ presenting symptoms not mentioned, only line of treatment given, supporting documentation vague or insufficient.
13. Claims with missing information like post-operative histopathology reports, surgical / anaesthetist notes missing in surgical cases.
14. Multiple claims with repeated hospitalization (under a specific policy at different hospitals or at one hospital of one member of the beneficiary family unit and different hospitals for other members of the beneficiary family unit,
15. Multiple claims towards the end of policy cover period, close proximity of claims.

Admissions Specific Triggers

16. Members of the same beneficiary family getting admitted and discharged together.
17. High number of admissions.
18. Repeated admissions.
19. Repeated admissions of members of the same beneficiary family unit.
20. High number of admission in odd hours.
21. High number of admission in weekends/ holidays.
22. Admission beyond capacity of hospital.
23. Average admission is beyond bed capacity of the provider in a month.
24. Excessive ICU (Intensive Care Unit) admission.
25. High number of admission at the end of the Policy Cover Period.
26. Claims for medical management admission for exactly 24 hours to cover OPD treatment, expensive investigations.
27. Claims with Length of Stay (LOS) which is in significant variance with the average LoS for a particular ailment.

Diagnosis Specific Triggers

28. Diagnosis and treatment contradict each other.
29. Diagnostic and treatment in different geographic locations.
30. Claims for acute medical Illness which are uncommon e.g. encephalitis, cerebral malaria, monkey bite, snake bite etc.
31. Ailment and gender mismatch.
32. Ailment and age mismatch.
33. Multiple procedures for same beneficiary – blocking of multiple packages even though not required.

34. One-time procedure reported many times.
35. Treatment of diseases, illnesses or accidents for which an Empanelled Health Care Provider is not equipped or empanelled for.
36. Substitution of packages, for example, Hernia as Appendicitis, Conservative treatment as Surgical.
37. Part of the expenses collected from beneficiary for medicines and screening in addition to amounts received by the Insurer.
38. ICU/ Medical Treatment blocking done for more than 5 days of stay, other than in the case of critical illnesses.
39. Overall medical management exceeds more than 5 days, other than in the case of critical illness.
40. High number of cases treated on an out-of-pocket payment basis at a given provider, post consumption of financial limit.

Billing and Tariff based Triggers

41. Claims without supporting pre/ post hospitalisation papers/ bills.
42. Multiple specialty consultations in a single bill.
43. Claims where the cost of treatment is much higher than expected for underlying etiology.
44. High value claim from a small hospital/nursing home, particularly in class B or C cities not consistent with ailment and/or provider profile.
45. Irregular or inordinately delayed synchronization of transactions to avoid concurrent investigations.
46. Claims submitted that cause suspicion due to format or content that looks "too perfect" in order. Pharmacy bills in chronological/running serial number or claim documents with colour photocopies. Perfect claim file with all criteria fulfilled with no deficiencies.
47. Claims with visible tempering of documents, overwriting in diagnosis/ treatment papers, discharge summary, bills etc. Same handwriting and flow in all documents from first prescription to admission to discharge. X-ray plates without date and side printed. Bills generated on a "Word" document or documents without proper signature, name and stamp.

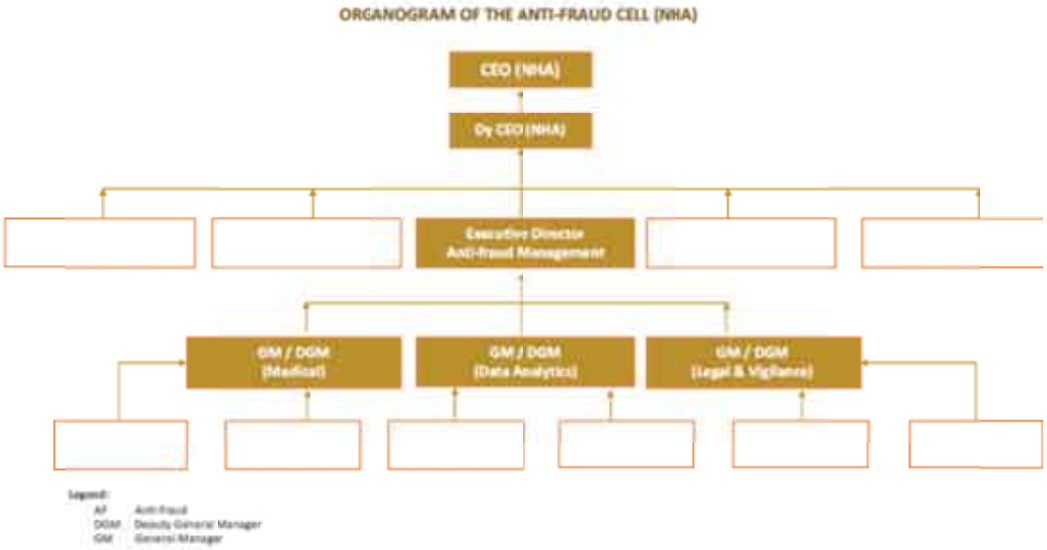
General

48. Qualification of practitioner doesn't match treatment.
49. Specialty not available in hospital.
50. Delayed information of claim details to the Insurer.
51. Conversion of out-patient to in-patient cases (compare with historical data).
52. Non-payment of transportation allowance.
53. Not dispensing post-hospitalization medication to beneficiaries.

Annex 3 Anti-Fraud Cell – Structure and Composition

At the National Health Agency (NHA)

It is proposed to establish an Anti-Fraud Management Cell as an independent vertical in NHA, headed by an Executive Director, reporting to Chief Executive Officer (NHA). Some of the roles/responsibilities may have some overlap with presently planned functions of Medical audit, grievance and vigilance teams, however it is felt that an independent anti-fraud vertical is critical for focused efforts and results in this area. The overlapping roles/functions, will be reviewed and streamlined to ensure synergies, avoid duplication of effort, and, for greater efficiency.



Positions, skills and key responsibilities:

Position	Education and skill set	Key responsibilities
ED Anti – fraud management	- Post graduate in medicine, management, legal, IT or equivalent discipline. - 10 years relevant experience in health insurance or 3-5 years' experience, in government administered health insurance scheme in key positions. - Director or equivalent level if in Govt job, others from private sector with 10 years' experience in leadership position.	- To develop vision, strategy, guidelines and implementation road map for robust fraud management under PMJAY from prevention, detection to deterrence, public awareness, whistle blower facilitation, etc. - To work with IT team for system integration, deployment of tools, advanced analytics etc. for fraud management. - To oversee SHA performance with regard to fraud management, guide, mentor and support capacity building in SHAs,

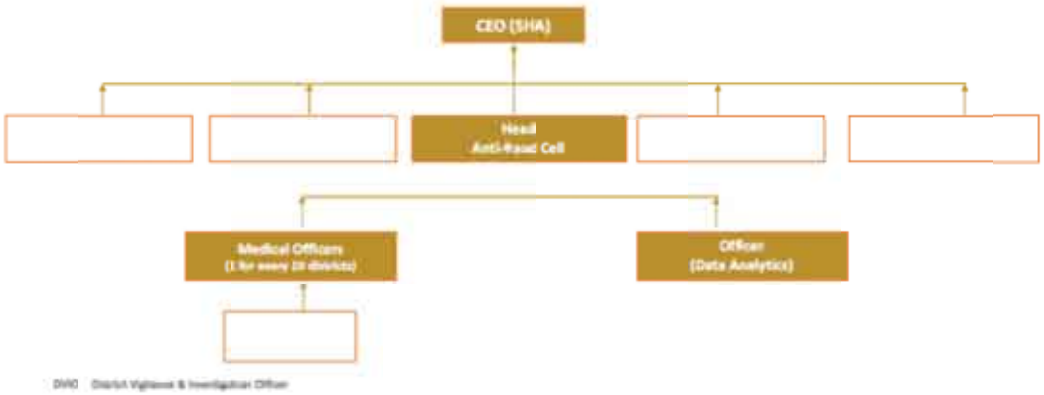
Position	Education and skill set	Key responsibilities
	- Leadership, communication, analytics, vigilance and medical forensics capability preferred.	standard training and certification programmes. - To work with legal, regulatory and industry bodies for standard contracts, punitive action, search, seizure, other deterrence measures/guidelines etc. - To develop strong zero tolerance anti-fraud culture in all aspects of the Scheme.
GM/DGM Medical	- Post graduate in medicine (recognized by MCI). - 10 years' experience, health insurance/schemes claims management/audit preferred. - Knowledge of medical protocols, standard treatment guidelines. - Presentation and communication skills.	- To work with IT team for embedding fraud triggers, medical protocols, guidelines and medical audit capabilities (concurrent & post facto) in the system. - To develop medical audit and check lists for SHA team, post audit action closure. - To analyze data, trends and ensure field investigations through vigilance team for outlier cases. - To guide, mentor, support SHA Medical team & oversee performance. - To carry out surprise field visits.
GM/DGM Analytics	- Post graduate in IT, statistics, management or equivalent. - 10 years' relevant experience - Knowledge of data mining, data consolidation, Big data, analytical tools and soft wares e.g. R, Weka, Tableau. - Strong analytical capability for large database behaviour, trends, predictive modelling etc. - Presentation and communication skills.	- To manage, organize and analyze transactions data - To manage, organize and analyze transactions data. - To work with IT team and develop dashboards for trend and behaviour, outlier cases. - To work with IT team for developing dynamic rule engines, triggers and predictive modelling. - To manage and update trigger list, publish the same for other teams and SHA's use. - To publish daily MIS and reports relating to anti-fraud management in coordination with Medical audit team for subsequent timely action. - To guide, mentor and support SHA Analytics team. - To work with Capacity Building team and Communications & Grievance Redressal Team to support development relevant

Position	Education and skill set	Key responsibilities
		training materials and IEC materials for SHAs.
GM/DGM Legal & Vigilance	- Post graduate, law degree. - 10 years' experience. - Criminal prosecution law back ground preferred. - Ex-servicemen preferred. - Strong investigative capabilities, communication skills.	- To lay guidelines, SOP and check lists for vigilance, field verification, investigation, conclusive evidence collection, etc. - To establish whistle blower mechanism at NHA level. - To develop strong vigilance and investigation capacity in the SHA team, develop training programmes. - To carry out surprise visits based on grievances, claims data, trends, M & E team inputs etc. - To develop a network of informal/extended community for discrete intelligence inputs and local issues. - To develop guidelines and SOPs for suitable action for dealing with fraud – contracts, legal and punitive action, prosecution, search, seizure, claw back recoveries etc. - To develop framework for deterrence measures guidelines. - To ensure compliance with anti-fraud guidelines as regards penalties and action. - To develop and deploy public awareness and social messaging guidelines/content for anti-fraud issues in consultation with IEC team including establishing social audits. - To guide, mentor and support SHA team.

At the State Health Agency (SHA)

For SHA, it is proposed to have a combined unit for Anti-fraud, medical audit and vigilance at the state level and to have Vigilance and Investigation Officers at district level. In case SHA is implementing scheme under insurance model or through Implementing Support Agency (ISA), the District Vigilance and Investigation Officer may be requisitioned from such insurance company or ISA as part of service level agreement, the positions need not be duplicated, however the structure in SHA is proposed to remain same.

ORGANOGRAM OF THE ANTI-FRAUD CELL (SHA)



Positions, skills and key responsibilities:

Position	Education and skill set	Key responsibilities
Chief Manager – Anti fraud, vigilance and legal	- Graduate, preferably law or forensics. - 10 years' experience. - Ex-servicemen/senior officials engaged in health insurance schemes implementation/hospital/social schemes implementation. - Good communication skills, analytical, investigative and forensics capabilities. - To carry out action – penalty, de-empanelment, prosecution, and other deterrence measures as per anti-fraud guidelines.	- To implement anti-fraud management guidelines laid down by NHA and additionally design/implement state specific guidelines, enforce contracts. - To guide, mentor and oversee District Vigilance officers, conduct training programmes. - To work with medical audit and analytics team for ensuring prompt and effective investigation of all suspect cases with collection of documentary evidence. - To develop anti-fraud messaging and public awareness campaigns in local languages along with the communication team, liaise with other state level regulatory bodies for

Position	Education and skill set	Key responsibilities
		concerted action, local officials, communities for intelligence. - To establish whistle blower mechanism. - To carry out surprise inspection. - To carry out action – penalty, de-empanelment, prosecution, and other deterrence measures, etc. as per guidelines against fraudsters.
Medical Officers (about 1 per 10 districts)	- Medical graduate. - 5-7 years' experience in health claims processing/audit. - Knowledge of medical protocols, clinical pathways and standard treatment guidelines. - Operational knowledge of hospital functioning and billing practices.	- To carry out medical audit as per guidelines incorporating state specific practices - To analyze transactions data from medical perspective and highlight. outlier/suspect/variant cases for further investigation. - To support investigation team for appropriate probing of suspect cases.
Data Analytics Officer	- Graduate, preferably Computer Science. - 5-7 years, preferably in MIS, reporting in volume business industry/health schemes. - Knowledge of data and query management, advanced analytics. - MIS and reporting.	- To apply fraud triggers to all transactions on daily basis and share report with Medical audit and Vigilance team. - Update triggers in the system based on new information. - To manage, organize and analyze state level data, compare utilization, average movement, length of stay, outlier cases etc. across providers, districts at micro and macro level. - To publish dashboard pertaining to anti-fraud work.

District Level

Position	Education and skill set	Key responsibilities
District Vigilance and Investigation Officer	- Graduate. - 3-5 years, preferably investigation related field jobs, ex-servicemen preferred. - Good communication skills, sharp and investigative mindset. - Knowledge of hospital billing practices desirable.	- To carry out field investigation of assigned cases within timeline, collecting documentary evidence. - To collect market intelligence reports discretely. - To carry out any other assigned tasks relating to anti-fraud management.

Annex 4 Measuring Effectiveness of Anti-Fraud Efforts

1. Share of pre-authorization rejected
2. Emergency pre-authorization as a share of total pre-authorisation requests
3. Share of pre-authorization and claims audited
4. Claim repudiation/denial/ disallowance ratio
5. Reduction in number of enhancements requested per 100 claims
6. Number of providers dis-empanelled
7. Share of combined/multiple-procedures per 100,000 procedures
8. Instances of single disease dominating a geographical area are reduced
9. Disease utilization rates correlate more with the community incidence
10. Share of households physically visited by PMJAY functionary
11. Reduction in utilization of high-end procedure
12. Number of enquiry reports against hospitals
13. Number of enquiry reports against own staff
14. Number of FIRs filed
15. Conviction rate of detected fraud
16. Number of cases discussed in Empanelment and Disciplinary Committee
17. Per cent of pre-authorisations audited
18. Per cent of post-payment claims audited
19. Fraudulent claims as a share of total claims processed
20. Number of staff removed or replaced due to confirmed fraud
21. Number of actions taken against hospitals in a given time period
22. Amount recovered as a share of total claims paid
23. Frequency of hospital inspection in a given time period in a defined geographical area
24. Share of red flag cases per 100 claims
25. Inter-district trends in incidence and utilisation rates
26. Number of fraud reported on helplines
27. Movement of averages: claim size, length of stay, etc.

Annexure 2: Fraud Risk Monitoring Framework by IRDAI

बीमा विनियामक और विकास प्राधिकरण
INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY

No.IRDA/SDD/MISC /CIR/ 009/ 01/2013 January 21, 2013

To CEOs of all Insurance and Reinsurance Companies

Insurance Fraud Monitoring Framework

A. Introduction:

Financial Fraud poses a serious risk to all segments of the financial sector. Fraud in insurance reduces consumer and shareholder confidence; and can affect the reputation of individual insurers and the insurance sector as a whole. It also has the potential to impact economic stability. It is, therefore, required that insurers understand the nature of fraud and take steps to minimize the vulnerability of their operations to fraud. Due measures also have to be laid down to address possible frauds in each line of business viz., life, general and health as threats/vulnerabilities posed under each one of them vary significantly.

Under the Regulatory Framework put in place for insurance companies, the Authority has stipulated a number of measures to be taken by insurance companies to address the various risks faced by them. Some of these include:

- The Corporate Governance guidelines mandate insurance companies to set up a Risk Management Committee (RMC). The RMC is required to lay down the company-wide Risk Management Strategy.
- As part of the Responsibility Statement which forms part of the Management Report filed with the Authority under the IRDA (Preparation of Financial Statements and Auditors' Report of Insurance Companies) Regulations, 2002, the management of an insurance company is required to disclose the adequacy of systems in place to safeguard the assets for preventing and detecting fraud and other irregularities, on an annual basis.

In order to provide regulatory supervision and guidance on the adequacy of measures taken by insurers to address and manage risks emanating from fraud, the Authority has laid down the guidelines requiring insurance companies to have in place the Fraud Monitoring Framework.

Page 1 of 6

Fraud Risk Management Systems for Reinsurer:

Reinsurers can reduce their exposure to fraudulent claims from ceding insurers and reinsurance intermediaries by understanding the fraud risk management systems these counterparties have in place. Accordingly, these guidelines apply *mutatis mutandis* in case of Reinsurers.

The Guidelines mandate insurance companies to put in place, as part of their corporate governance structure:

(i) fraud detection and mitigation measures; and
(ii) submit periodic reports to the Authority in the formats prescribed herein.

All insurers are required to ensure that the risk management function is organized in such a way that the insurer is able to monitor all the risks across all lines of business on a continuing basis and to initiate measures to address them suitably.

B. Scope and Classification of Insurance Frauds:

Fraud in insurance is an act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other related parties. This may, for example, be achieved by means of:

- misappropriating assets;
- deliberately misrepresenting, concealing, suppressing or not disclosing one or more material facts relevant to the financial decision, transaction or perception of the insurer's status;
- abusing responsibility, a position of trust or a fiduciary relationship.

In order to adequately protect itself from the financial and reputational risks posed by insurance frauds, every insurance company shall have in place appropriate framework to detect, monitor and mitigate occurrence of such insurance frauds within its company. The said framework shall, at the minimum, include measures to protect the insurer from the threats posted by the following broad categories of frauds:

a) *Policyholder Fraud and/or Claims Fraud* - Fraud against the insurer in the purchase and/or execution of an insurance product, including fraud at the time of making a claim.

b) *Intermediary Fraud* - Fraud perpetuated by an insurance agent/Corporate Agent/intermediary/Third Party Administrators (TPAs) against the insurer and/or policyholders.

c) *Internal Fraud* – Fraud/ mis-appropriation against the insurer by its Director, Manager and/or any other officer or staff member (by whatever name called).

An illustrative list of Insurance Frauds is given at Appendix – 1. These instances include frauds perpetuated internally; by insurance agent/Corporate Agent/intermediary/TPAs; and instances of claims/policyholder frauds.

For more examples please refer to http://www.iaisweb.org

C. Anti-Fraud Policy:

All insurance companies are required to have in place an Anti Fraud Policy duly approved by their respective Boards. The Policy shall duly recognize the principle of proportionality and reflect the nature, scale and complexity of the business of specific insurers and risks to which they are exposed. While framing the policy, the insurance company should give due consideration to all relevant factors including but not limited to the orgainsational structure, insurance products offered, technology used, market conditions, etc. As fraud can be perpetrated through collusion involving more than one party, insurers should adopt a holistic approach to adequately identify, measure, control and monitor fraud risk and accordingly, lay down appropriate risk management policies and procedures across the organization.

The Board shall review the Anti Fraud Policy on atleast an annual basis and at such other intervals as it may be considered necessary.

The anti-fraud policy shall broadly cover the following aspects:

i. Procedures for Fraud Monitoring:

Well-defined procedures to identify, detect, investigate and report insurance frauds shall be laid down. The function of fraud monitoring shall be either an independent function or can be merged with existing functions like risk, audit etc., The Head of this function should be placed at sufficiently senior management level and should be able to operate independently.

ii. Identify Potential Areas of Fraud:

Identify areas of business and the specific departments of the organization that are potentially prone to insurance fraud and lay down a detailed department-wise, anti-fraud procedures. These procedures should lay down the framework for prevention and identification of frauds and mitigation measures.

iii. Co-ordination with Law Enforcement Agencies:

Lay down procedures to coordinate with law enforcement agencies for reporting frauds on timely and expeditious basis and follow-up processes thereon.

iv. Framework for Exchange of Information:

Lay down procedures for exchange of necessary information on frauds, amongst all insurers through the Life and General respective councils. The insurance companies are well advised to establish coordination platforms through their respective Councils and/or Forum to establish such information sharing mechanisms.

v. Due Diligence:

Lay down procedures to carry out the due diligence on the personnel (management and staff)/ insurance agent/ Corporate Agent/ intermediary/ TPAs before appointment/ agreements with them.

vi. Regular Communication Channels:

Generate fraud mitigation communication within the organization at periodic intervals and/or adhoc basis, as may be required; and lay down appropriate framework for a strong whistle blower policy. The insurer shall also formalize the information flow amongst the various operating departments as regards insurance frauds.

D. Fraud Monitoring Function (FMF):

The FMF shall ensure effective implementation of the anti-fraud policy of the company and shall also be responsible for the following:

i. Laying down procedures for Internal reporting from/and to various departments.

ii. Creating awareness among their employees/ intermediaries/ policyholders to counter insurance frauds.

iii. Furnishing various reports on frauds to the Authority as stipulated in this regard; and

iv. Furnish periodic reports to their respective Board for its review.

E. Reports to the Authority:

The statistics on various fraudulent cases which come to light and action taken thereon shall be filed with the Authority in forms FMR 1 and FMR 2 providing details of

(i) outstanding fraud cases; and
(ii) closed fraud cases

every year within 30 days of the close of the financial year.

F. Preventive mechanism:

The Insurer shall inform both potential clients and existing clients about their anti-fraud policies. The Insurer shall appropriately include necessary caution in the insurance contracts/ relevant documents, duly highlighting the consequences of submitting a false statement and/or incomplete statement, for the benefit of the policyholders, claimants and the beneficiaries.

G. Insurer's to Ensure Compliance:

The stipulations on fraud detection, classification, monitoring and reporting by the insurers shall be effective from the financial year 2013-14. A compliance certificate confirming laying down of appropriate procedures shall be submitted by 30th June 2013.

(J. HARI NARAYAN)
Chairman

Appendix – 1

Illustrative List of Insurance Frauds

Broadly, the potential areas of fraud include those committed by the officials of the insurance company, insurance agent/corporate agent/intermediary/TPAs and the policyholders/ their nominees. Some of the examples of fraudulent acts/omissions include, but are not limited to the following:

1. Internal Fraud:

   a) misappropriating funds
   b) fraudulent financial reporting
   c) stealing cheques
   d) overriding decline decisions so as to open accounts for family and friends
   e) inflating expenses claims/over billing
   f) paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
   g) permitting special prices or privileges to customers, or granting business to favoured suppliers, for kickbacks/favours
   h) forging signatures
   i) removing money from customer accounts
   j) falsifying documents
   k) selling insurer's assets at below their true value in return for payment.

2. Policyholder Fraud and Claims Fraud:

   a) Exaggerating damages/loss
   b) Staging the occurrence of incidents
   c) Reporting and claiming of fictitious damage/loss
   d) Medical claims fraud
   e) Fraudulent Death Claims

3. Intermediary fraud:

   a) Premium diversion-intermediary takes the premium from the purchaser and does not pass it to the insurer
   b) Inflates the premium, passing on the correct amount to the insurer and keeping the difference
   c) Non-disclosure or misrepresentation of the risk to reduce premiums
   d) Commission fraud - insuring non-existent policyholders while paying a first premium to the insurer, collecting commission and annulling the insurance by ceasing further premium payments.

***

FMR – 1

Fraud Monitoring Report

Name of the Insurer:
Report for the year ending

Part I

Frauds Outstanding- Business segment wise *:

Sl. No.	Description of Fraud	Unresolved Cases at the beginning of the year		New cases detected during the year		Cases closed during the year		Unresolved Cases at the end of the year	
		No.	Amount involved (₹ lakh)	No.	Amount involved (₹ lakh)	No.	Amount involved (₹ lakh)	No.	Amount involved (₹ lakh)
	Total								

Part II

Statistical details: (unresolved cases as at end of the year) –Business segment wise*

Sl. No.	Description of Fraud	No. of Cases	Amount Involved (₹ lakh)
	Total		

Part III

Preventive and Corrective steps taken during the year- Business segment wise*

Sl.No.	Description of the fraud	Preventive/Corrective action taken

Part IV

Cases Reported to Law Enforcement Agencies

Sl. No.	Description	Unresolved Cases at the beginning of the year		New cases reported during the year		Cases closed during the year		Unresolved cases at the end of the year	
		No.	₹ lakh	No.	₹ lakh	No.	₹ lakh	No.	₹ lakh
	Cases reported to Police								
	Cases reported to CBI								
	Cases reported to Other agencies (specify)								
	Total								

* Business segments shall be as indicated under IRDA (Preparation of Financial Statements and Auditor's Report of Insurance Companies) Regulations, 2002

CERTIFICATION

Certified that the details given above are correct and complete to the best of my knowledge and belief and nothing has been concealed or suppressed.

Date:
Place:

Signed/-
Name of the Chief Executive Officer of the Insurer

FMR – 2

Fraud Cases closed during the year

Name of the Insurer: Report for the year ending

Sl. No.	Basis of closing a case	Number of cases closed
1.	The fraud cases pending with CBI/Police/Court were finally disposed off	
2.	The examination of staff accountability has been completed	
3.	The amount involved in the fraud has been recovered or written off	
4.	The insurer has reviewed the systems and procedures; identified the causative factors; has plugged the lacunae; and the portion taken note of by appropriate authority of the insurer (Board, Committee thereof)	
5.	Insurer is pursuing vigorously with CBI for final disposal of pending fraud cases, staff side action completed. Insurer is vigorously following up with the police authorities and/or court for final disposal of fraud cases	
6.	Fraud cases where: The investigation is on or challan/ charge sheet not filed in the Court for more than three years from the date of filing of First Information Report (FIR) by the CBI/Police; or Trial in the courts, after filing of charge sheet / challan by CBI / Police has not started, or is in progress.	

CERTIFICATION

Certified that the details given above are correct and complete to the best of my knowledge and belief and nothing has been concealed or suppressed.

Date:
Place:

Signed/-
Name of the Chief Executive Officer of the Insurer

Closure of Fraud Cases:

For reporting purposes, only in the following instances of fraud cases can be considered as closed:

1. The fraud cases pending with CBI/Police/Court are finally disposed of.
2. The examination of staff accountability has been completed
3. The amount of fraud has been recovered or written off.
4. The insurer has reviewed the systems and procedures, identified the causative factors and plugged the lacunae and the fact of which has been taken note of by the appropriate authority of the insurer (Board / Audit Committee of the Board)
5. Insurers are allowed, for limited statistical / reporting purposes, to close those fraud cases, where:

    a. The investigation is on or challan/ charge sheet not filed in the Court for more than three years from the date of filing of First Information Report (FIR) by the CBI/Police, or
    b. The trial in the courts, after filing of charge sheet / challan by CBI / Police, has not started, or is in progress.

Insurers should also pursue vigorously with CBI for final disposal of pending fraud cases especially where the insurers have completed the staff side action. Similarly, insurers may vigorously follow up with the police authorities and/or court for final disposal of fraud cases and / or court for final disposal of fraud cases.

Annexure 3: Definition of Fraud used in different countries' Healthcare Programs

Indonesia

Indonesia's ministerial decree (*Permenkes No. 36 Tahun 2015)* defines fraud as "intentional act committed by participants, health BPJS Staff, health service providers and medicine and medical device suppliers to take financial advantage of health security programs under the National Social Security System through illicit fraudulent activities." The decree recognizes several types of fraud:

Beneficiaries: (a) making a false statement of eligibility (falsifying membership status) to access health services; (b) using their rights to unnecessary services by falsifying their health conditions; (c) giving gratifications to service providers to provide excluded/uncovered services; (d) manipulating income to reduce contribution payments; (e) engaging in a conspiracy with service providers to submit false claims; (f) receiving prescribed medicines and/or medical devices for resale

BPJS staff: (a) engaging in a conspiracy with participants and/or health facilities to submit false claims; (b) manipulating uncovered benefits into covered benefits; (c) suspending payments to health facilities/partners to take personal advantage; (d) paying capitation amounts different from the stipulation

Fraud by service providers: (a) using capitation funds in ways inconsistent with laws and regulations; (b) manipulating claims for services paid through a non-capitation mechanism;

(c) receiving a commission for referral to higher-level facilities; (d) collecting fees from participants already covered by capitation and/or non- capitation fees according to the standard rates specified; (e) giving patients an inappropriate referral to gain a particular advantage; (f) diagnosis upcoding; (g) cloning of claims from other patients; (h) phantom billing; (i) inflated bills for medicines and medical devices; (j) services unbundling or fragmentation; (k) self-referral; (l) repeated billing; (m) prolonged length of stay; (n) manipulating types of room charge; (o) cancelled services; (p) measures of no medical value; (q) deviation from the standard of care; (r) unnecessary treatment; (s) extended time for use of ventilators; (t) phantom visits; (u) phantom procedures; (v) readmissions; and (w) seeking cost- sharing inconsistent with laws and regulations

The Philippines

The Implementing Rules and Regulations (IRR) of the National Health Insurance Act of 2013 distinguishes fraudulent and non-fraudulent acts that health care facilities, health care providers and members can commit. Both non-fraudulent and fraudulent acts have corresponding penalties, with the latter having stricter penalties. The IRR also enumerates the following as fraudulent acts: *padding of claims, extending the period of confinement, post-dating of claims, misrepresentations, fabrication, or possession of fabricated forms*.

The United States

CMS has issued numerous technical reports that defines fraud and its differences from abuse, waste, and error. Any of the following broadly constitute fraud:

-Knowingly submitting, or causing to be submitted, false claims or making misrepresentations of fact to obtain a federal health care payment for which no entitlement would otherwise exist

-Knowingly soliciting, receiving, offering, and/or paying remuneration to induce or reward referrals for items or services reimbursed by federal health care programs

-Making prohibited referrals for certain designated health services

These operational definitions of fraud are clearly described in the following federal laws:

-Anti-Kickback Statute

-Criminal Healthcare Fraud Statute

-Physician Self-Referral Law (or Stark Law)

-False Claims Act

-Social Security Act

Sources: Ministry of Health (Indonesia), PHIC, and CMS

Annexure 4 – Anti-fraud provisions in Provider contracts in different countries' healthcare programs

The following are some excerpts related to fraud in insurer-provider contracts.

Indonesia

BPJS (FIRST PARTY) and health care providers (SECOND PARTY) enter into a legal contract agreement, which clearly specifies the scope of function, and the rights and obligations of each party. The following are some of the provisions of the contract agreement relevant to fraud:

"if the claim bills of the SECOND PARTY are problematic, then the FIRST PARTY is entitled to suspend claims in question"

"in the case of SECOND PARTY is proven to actually do things as follows: (1) does not serve the Participant in accordance to obligations; (2) does not provide facilities and health services to Participants in accordance with the rights of Participants; collect additional fees to Participants outside the provisions, the FIRST PARTY shall be entitled to write a reprimand to the SECOND PARTY as many as 3 times with respective grace period of each letter..."

"In the event that one party is found to be abusing authority by conducting moral hazard or fraud (e.g., fictitious claims) as evidenced by the result of examination of the internal audit team, the injured party can cancel this agreement unilaterally"

The United States

CMS enters into a legal contract with a health care provider. The first section of the contract contains the definition of fraud and abuse:

"Fraud - An intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to himself or some other person. It includes any act that constitutes Fraud under applicable federal or state law."

In the Responsibilities section, the contract also includes an explicit provision against fraud: "<Provider> is subject to all state and federal laws and regulations relating to Fraud, Waste, and Abuse in health care and the Medicaid and Medicare programs. <Provider> must cooperate and assist CMS, the HHSC Office of Inspector General (OIG), and any state or federal agency charged with the duty of identifying, investigating, sanctioning or prosecuting suspected Fraud, Waste, or Abuse"

"Articulate the <Provider>"s commitment to comply with all applicable federal and state standards, including: (i) Fraud detection and investigation; (ii) Procedures to guard against Fraud, Waste, and Abuse; (iii) Prohibitions on certain relationships as required by 42 C.F.R. § 438.610; (iii) Obligation to suspend payments to Providers; (iv) Disclosure of ownership and control of<Provider>; (v) Disclosure of business transactions"

Turkey

SGK enters into a legal contract with a health care provider. The following are relevant excerpts from the contract:

"The parties to this contract: SGK and <name of private health service provider>. The basis of this contract is Article 73 of the Law 5510 and the Hizmet Regulation on the Preparation and Implementation of Health Service Procurement Agreements / Protocols of the Social

Security Institution 55 published in the Official Gazette dated 26/03/2016 and numbered 29665."

The contract stipulates the responsibilities that the providers need to abide such as documentary requirement during submission of claims and an agreement to allow SGK to conduct audit.

Sources: Ministry of Health (Indonesia), CMS, and SGK.

** *PREVENTING, DETECTING AND DETERRING FRAUD IN SOCIAL HEALTH INSURANCE PROGRAMS: LESSONS FROM SELECTED COUNTRIES, WB Discussion Papers, November 2018*

Annexure 5: Data Schema and Repository Structure

Section Details	Field Name	Field Description	Data Type	FRMP fields related to Fraud Identification	Exchange of fields permitted
Patient Details	Card Number	Unique card number allotted during enrollment	String	Policy Number	□
	Patient Family ID	Unique family identification number allocated to the family	String		
	Patient Name	This is the name of the patient	String	Name of the Insured	x*
	Patient Age	Age of the patient	Number		
	Patient Gender	Gender of the patient	String		

	Patient ID Type		Unique Govt. recognized ID like PAN, Voter ID, Aadhar Ration Card. We will need to get this data from BIS where the card number is generated.	Drop down. Allowed Values: - PAN - Aadhar Card - Voter ID - Ration Card - Driving License - Birth Certificate - Others	
	Patient ID Number	The unique ID number based on the Patient ID Type	String		
	Patient Address	The current address of the patient. We will break the address in to granular level to capture city, district, block, state code and pin code which is presently prevalent in BIS	String		

Entity Details on whom fraud is reported	Entity Name	Name of the entity involved in the fraud	String	Individual Name /Company as applicable	□
	Entity ID	ID Number of the entity involved in the fraud	String		
	Entity Id Type	The Govt recognized ID like Aadhar card, PAN etc.	Drop down. Allowed Values: - PAN (Applicable to Individual & company) - Aadhar Card - Voter ID - Ration Card - Driving License - Birth Certificate - Passport - Registration	ID Type (Voter ID/ Aadhar/PAN Card etc.)	□

			number/CIN - GST Number - Others		
	Entity Identification Number	The identification number based on the ID Type	String	ID Number	□
	Fraudster Type	Field to depict type of fraudster	Drop down. Allowed Values: - Individual - Organization - Others	Fraudster type – Individual/ Organization	□
	Fraudster Category	To differentiate the fraud into distinct categories	Drop down Allowed Values: - Provider - Internal Insurer member - Policyholder	Fraudster category (Doctor/ Hospital/Employee etc.)	□

			- Beneficiary - Intermediary - Payer Fraud - Others		
	Fraudster Sub Category	To bifurcate the Fraud Categories into further sub-categories	Drop down Allowed Values: For 'Provider' - - Hospital - Medical Practitioner - Diagnostic Centre - Pharmacy - PMAM - Others For 'Internal member' Fraud - - Board Member / Senior Management - Mid-Management Member - Other employee For 'Beneficiary' -		□

			- Patient admitted in hospital - Individual impersonating as beneficiary For 'Intermediary' - - Insurance Agent - Corporate Agent - CSC/VLE - Others For 'Payer Fraud' - - Insurance Company - TPA - PMAM - Support Agency - IT provider - Monitoring Agency - Others	

	Fraud Classification	To depict the classification of fraud committed	Drop Down Allowed Values: - Clinical fraud - Impersonation fraud - Counterfeiting - Misappropriation - Concealment - Cheating - forgery - Falsification - Criminal Breach of Trust - breach of contract - Others	
	Fraud Sub Classification	To bifurcate the Fraud classification into further sub-categories	Drop Down Allowed Values: - Unbundling - Upcoding - Phantom patients - Billing for services not provided	

			- Off label marketing of pharmaceuticals - Physician self-referrals - Kickbacks - Accepting bribes - Identity switch - Prescription Fraud - Not providing all services as charged or early discharge - Doctor switching - Non-licensed hospitals - Non-registered doctors - Others		
	Entity Contact Number	Mobile or landline number of that entity	String	Contact Number	□
	Entity Address	Full Address of the entity including the state and district and pin	String	Address details with Pin code	□

		code			
	Entity Latitude	The Geo location of the entity	String		
	Entity Longitude	The Geo location of the entity	String		
	Hospital Director1	Name of the Director of the hospital under consideration	String		
	Hospital Director ID1		The Govt recognized ID like Aadhar card, PAN etc.	Drop down. Allowed Values: - PAN - Aadhar Card - Voter ID - Ration Card - Driving License - Birth Certificate - Others	
	Hospital Director Number1	The identification number based on the ID Type	String		

	Hospital Director2	Name of the Director of the hospital under consideration	String		
	Hospital Director ID2		The Govt recognized ID like Aadhar card, PAN etc.	Drop down. Allowed Values: - PAN - Aadhar Card - Voter ID - Ration Card - Driving License - Birth Certificate - Others	
	HospitalDirectorNumber2	The identification number based on the ID Type	String		
Suspicion Indicator Details	Case No.	Case number which is reported in the fraud	String	Claim Number	□

	Fraud Index	To categorize the fraud into confirmed, unconfirmed and suspicious.	Drop Down. Allowed Values: - Suspicious - Confirmed - Unconfirmed	Where suspected or confirmed or unconfirmed (after investigation)	□
	Fraud Description	Description of the underlying trigger that has caused the suspicion	Free Text		
	Modus Operandi	A field depicting the underlying mechanism/method employed by the fraudsters to bring about the fraud	Free Text	Modus Operandi in Brief	□
	Existing Legal Case Indicator	To depict if any legal case is pending against the entity involved in the fraud or if any FIR was	Drop Down. Allowed Values: - Yes - No	Any Legal Case Pending	□

		lodged. This field will mainly have a Boolean value: YES or NO			
	Existing Legal Case Details	If the Existing Legal Case Indicator is YES; then this field would provide the details of the same.	Free Text	Legal Case Details	□
	Watch List Indicator Hosp	To indicate if the claim is registered against a hospital which is on the watchlist or on the radar for scrutiny. This field will mainly have a Boolean value: YES or NO	Drop Down. Allowed Values: - Yes - No		□

	Name of Insurer/Trust	Name of the insurer or trust. Here it doesn't imply that they are involved in fraud; but it is mainly to capture that information for further use	String	Name of Insurer	□
	Claim History Indicator		To indicate if any previous claims of the patient or the underlying family were rejected based on the Card No. or patient family ID	Drop Down. Allowed Values: - Yes - No	
	Claim History Count	To indicate the count where the claim was rejected previously for this person	Number		
	Claim History Date	If the Claim History Indicator is YES; the date when last claim	Date Type		

		was rejected			
Investigation/ Detection And Actions Taken	Investigator Type		This is mainly to cater to the type of investigator that will be assigned here	Drop Down Allowed Values: - Internal Investigator - External Investigator - Internal and External investigator - Industry Collaboration - Others	
	Investigator Name	Name of the person or agency assigned for investigating the claim	String		
	Investigation Type		To depict the type of investigation	Drop Down Allowed Values: - On-field investigation - Investigation via call centres - Others	

	Suspicion Reported Date	The Date when the suspicion was first raised	Date Type		□
	Fraud Confirmed Date	The Date when the underlying case was confirmed as fraud	Date Type	Year of detection of fraud	□
	Action since confirmed	To indicate action taken against the entity after fraud is confirmed	Drop Down - Allowed values: De-empaneled, Intermediary barred, Claim denied, Money recovered, FIR lodged, Reported to MCI/State Medical Establishment Act, Included in Name & Shame, Industry blacklisted, Hospital registration cancelled, Others		□
	Date of Action	To indicate date when action is taken against the entity	Date Format		
	Time Period of Action	the time period for which the Action is valid	Numeric in Months		

	Amount Recovered	The amount that was recovered from the entity involved in fraud as a part of the action	Drop Down Allowed values - Claim amount Rs.____, - Penalty Amount Rs._____, - Others Rs.____		□
Other Details	Hospital Type	To indicate if this hospital is Public or a privately owned in case of hospital being the entity.	Drop Down Allowed Values: - Public Hospital - Private Hospital - Private Charitable Hospital - Others		□
	ROHINI ID	ROHINI ID assigned to hospitals by IRDA	String		□
	Preauth Initiated Date	Date when the preauthorizatio n was initiated	Date Type	Claim Details	□
	Preauth Approved Date	Date when the preauthorizatio n was approved	Date Type		

	Preauth Approved Amount	The amount that has been approved for Preauth	String		
	Claim Amt	The amount initiated for this Case No.	String		
	Claim Submitted Date	The date when the claim was submitted	Date Type		
	Claim Paid Date	The amount that was approved to be paid for this case number	Date Type		
	Claim Reject Date	Date when the claim was rejected	Date Type		
	Claim Reject Reason	The reason for rejecting a part or full claim	String		
	Case Status	The status of the claim. This is prevalent in the form of workflow status in AB schema	String	Claim Status	□

	Date Of Admission	Field to capture Admission Date	DateType	Case Details	□
	Date Of Discharge	Field to capture Discharge Date	DateType		
	Hospital Specialty	The specialties prevalent in that hospital denoted by specialty code	String		
	Procedure Code	In case of PMJAY there are around 1393 packages which have been categorized as procedures which are again state specific	String		
	Procedure Name	Name of the procedure code	String		
	Diagnosis Code	ICD code	String		

	Diagnosis Name	Name of the diagnosis code	String		
	Treating Doctor Name	Name of the treating doctor	String		□
	Treating Doctor Reg	Registration number of the treating doctor	String		□
	Overall Remarks	A free text field to put any specific comments/remarks for the underlying case in consideration	String	Remarks	□

Annexure 6: Standard Format for Investigation

Investigation Category	Investigation Check point		Available with IC/ TPA/ ISA	Obtained by the investigator	Conclusion	Attach Document
Member verification	Name of the insurer/Beneficiary	Alpha				
	Address of Insured/beneficiary	Alpha numeric				
	Standard of Living	Alpha				Upload document
	Presenting Complaints (symptoms and duration)	Alpha				
	Customer Knowledge about ongoing Treatment	Yes/No				
	If yes, Treatment Advised	Alpha				
	Whether admitted or OPD or day care	Admitted/ OPD/ day care				

	Has any other family member undergo treatment in the past or recently ? Line of treatment, place of treatment	Alpha				
	Did the patient receive the PMJAY card, medical documents including discharge summary and reports at the time of discharge	Alpha				
	Name of the Hospital	Alpha numeric				
	Date & Time of Admission	DD/MM/YY hr: min				
	Date & Time of Surgery	DD/MM/YY hr: min				
	Date & Time of Discharge	DD/MM/YY hr: min				
	Scar Mark (wherever necessary)	alpha				

	Did the member/Beneficiary left hospital during the course of treatment ?	Yes/No				
	If yes, specify reasons	Hospital asked for money/Patient was not happy with the treatment/ Personal reasons/ Forced to leave/ Other				
	if others, specify reasons	alpha				
	Hospital Registration Details/ Certificate	Alpha numeric				
	Date of Registration	dd/MM/YY				
	Rohini Id	Alpha numeric				
Hospital	Patient Registration	Alpha				Name, registration

verification	Details- PMJAY id	numeric				no.
	Treating Doctor's Verification	Alpha numeric				ID no, qualification, Specialisa-tion
	Discharge summary available	Yes/No				Collect discharge summary
	ICP records available	Yes/No				Upload ICP, medical, OT, Vital charts, treatment notes, ABG report in case of patient on ventilator
	- ICP's in line with the Diagnosis & Treatment	yes/no/ refer to Medical Doctor				
	- Does ICP's reflect any Exclusion under the Scheme/similar handwriting/	yes/no/refe r to Medical Doctor				

	overwriting/ tampering/ duration					
	Does the hospital infrastructure commensurate with the treatment given ?	Yes/No				
	Hospital Infrastructure/ facilities are clean and upto the mark? Check -Lab/ Operation Theater/ Oxygen Cylinder/Pharmacy/ No. of Beds / general ward/nursing staff, round the clock doctor	Alpha numeric/ drop down				Collect details
	FIR/ MLC (in case of hospitalization due to unnatural causes)	Yes/No				Upload document
	Pathology Register available	Yes/No				Upload evidence of pathology tests

	Radiology Register available	Yes/No				Upload evidence of radiology tests
	OPD register available	Yes/No				Upload evidence of OPD details
	IPD register available	Yes/No				Upload evidence of IPD details
	OT register available	Yes/No				Upload evidence of OT details
	Any other Observation (suspicious flagging/ marking)	Alpha numeric				Upload evidence wherever available
Member verification	PMJAY ID No.					
	Aadhaar card available	Yes/No				Upload Aadhaar copy
	If Aadhaar card not available any other Govt Photo id proof	Voter's id/Driving license/ Pan card /Birth Certificate				

	Id no.	alpha numeric				Upload document
	PMJAY Card Verification / Photo Matching and Any One Govt. Photo ID proof	Alpha				
	Is aware that Treatment under PMJAY is free of Cost	Yes/No				
	Previous Treatment under this Scheme (Details) if any	Alpha				
	Did the beneficiary undergo any medical tests post surgery?	Yes/No				
	Did the beneficiary get Post discharge medicines from Hospital	Yes/No				
	If yes, how many days	Numeric				
	Amount paid for availing treatment of current ailment	Numeric				

	under PM-JAY scheme					
	If yes, for what did you pay for ?	Treatment/ tests/food/ medication				
Member verification	Name and any Govt. photo id proof Policyholder (If Member and policyholder are different)	Alpha				Upload document
	Relationship with Policyholder	Drop down (relation-ships)				
	Any other claim from a Group/Individual policy	Yes/No				Upload document wherever available
	First Consultation papers & Reports	Yes/No				Upload document wherever available
	Follow Up Consultation Papers & test reports	Yes/No				Upload document wherever available

Hospital verification	Hospital Registration Details/ Certificate	Yes/No				Upload document wherever available
	Hospital Tariff Details	Yes/No				Upload document wherever available
	Pathologist/ Radiologist Verification	Alpha				
	Medicine Purchase Invoice Verification/ Stock Register	Alpha numeric				Upload document
	Distance Between Patient Residence and Hospital in Kms	Numeric				
Other Checks	Employer Check, Leave records & Any mediclaim facilities availed by member	Alpha numeric				Upload document
	Verification from insured's neighbors	Yes/No				Upload document
	Verification from other nearby	Yes/No				Upload document

	hospitals, Diagnostic centers, pharmacies					
	Family Physician Check	Yes/No				Upload document
	Claims from other insurance Companies	Yes/No				Upload document
	Is Hospital/ Doctors/Diagnostic center tagged suspicious ?	Yes/No				Upload document
	Is insured tagged suspicious ?	Yes/No				Upload document

Annexure 7: Name & Shame - Legal implications and International Examples

Legal implication related to Naming and Shaming: Banking sector

In the banking industry, the financial indiscipline in the banking sector in India has led to escalation of bad loans which prompted passing of the Recoveries of Debts due to Banks and Financial Institutions Act, 1993 (DRT Act) and Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 (SARFAESI Act).

However, the right of the banks to adopt any lawful method for the recovery of its dues, including the publication of the photograph of the defaulter has come directly into conflict with right to privacy and dignity of the borrower, which is a part of the right to life guaranteed under article 21 of the Constitution of India. The Supreme Court of India in R. Rajagopal Vs. State of Tamil Nadu and PUCL Vs. UOI has eloquently interpreted the right to privacy as an implicit right in the right to life.

Moreover, right to privacy is expressly mentioned in Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which provides protection to personal information.

Even under International law, the right to privacy has been protected in a number of conventions such as the Universal Declaration of Human Rights, 1948 (UDHR) which provides that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."(Article 12)

Legal precedent and Judicial Opinion on Naming and Shaming:

Different perspective of Courts on the matter of publication of willful defaulter list by lending Bank:

In Metsil Exports Private Ltd. & Anr Vs. Punjab National Bank & Anr, 2016, the Calcutta High Court has taken the view that the bank had grossly exceeded its authority in publishing the demand notice in the newspapers along with the photograph of the defaulter and directed the bank to publish an apology in the newspapers.

In the matter of P.R. Venu Vs. State Bank of India, 2013, Kerala High Court came down heavily upon the banks observing that the practice of exhibiting a photograph of a person and shaming him in public for the sin of being in an impecunious condition cannot be encouraged in a civilized society like ours.

Contrarily, Chhattisgarh High Court in Mohan Products Pvt. Ltd. & Others Vs. State Bank of India, 2015, held that Rule 8 clearly demonstrates that the Bank has the right to publish the name of defaulters and that publication of photograph has got legal sanction under Rule 8 (6) (f) of the SARFAESI Rules, 2002.

International Examples

NHS, UK

The government in England sought to change the system of perverse incentives that had developed across the different countries: from one that ignored success and rewarded failure to one that celebrated success and penalized failure. This was done through the radical and controversial system of annual `star rating' of NHS organizations, between 2001 and 2005, which `named and shamed' those that `failed', which were zero rated; and offered `earned autonomy' to the `high-performing' three-star organizations. The results show that this was indeed effective in bringing down the waiting times in England

The U.S. Department of *Health and Human Services* (*HHS*)

To get healthcare's powerful players to behave as desired, HHS and its various units are increasingly turning to the same playbook: naming and shaming bad actors. Most recently, the CMS and the Office of the National Coordinator for Health Information Technology issued two proposed rules to spur interoperability and counter information-blocking.

Among the rule's provisions is to post a list online of healthcare clinicians and hospitals that block the transfer of patient information, with the goal of getting providers to curb the practice make patient information available in a standard, easily manipulated format.

The strategy of naming bad actors has also been used in the administration's efforts to curb high drug prices. The CMS and the Food and Drug Administration have sought to name drug companies that raise prices too high on Medicare engage in anti-competitive tactics to deter generic-drug competition.

Annexure 8: Relevant MCI Regulations

Chapter 7

"7. MISCONDUCT: The following acts of commission or omission on the part of a physician shall constitute professional misconduct rendering him/her liable for disciplinary action

7.7 Signing Professional Certificates, Reports and other Documents:

Any registered practitioner who is shown to have signed or given under his name and authority any such certificate, notification, report or document of a similar character which is untrue, misleading or improper, is liable to have his name deleted from the Register."

Chapter 8

8. PUNISHMENT AND DISCIPLINARY ACTION

8.1 It must be clearly understood that the instances of offences and of Professional misconduct which are given above do not constitute and are not intended to constitute a complete list of the infamous acts which calls for disciplinary action, and that by issuing this notice the MCI and or State Medical Councils are in no way precluded from considering and dealing with any other form of professional misconduct on the part of a registered practitioner. Circumstances may and do arise from time to time in relation to which there may occur questions of professional misconduct which do not come within any of these categories. Every care should be taken that the code is not violated in letter or spirit. In such instances as in all others, the MCI and/or State Medical Councils have to consider and decide upon the facts brought before the MCI and/or State Medical Councils.

This act of commission also falls within the purview of 'Falsification of documents' as defined under Section 477-A and Section 464 of Indian Penal Code (IPC).

1.'IPC Section 464. Making a false document'

A person is said to make a false document-

First- Who dishonestly or fraudulently makes, signs, seals or executes a document or part of a document, or makes any mark denoting the execution of a document, with the intention of causing it to be believed that such document or part of a document was made, signed, sealed or executed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed or executed, or at a time at which he knows that it was not made, signed, sealed or executed; or Secondly- Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document in any material part thereof, after it has been made or executed either by himself or by any other person, whether such person be living or dead at the time of such

alteration; or Thirdly- Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document, knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, he does not know the contents of the document or the nature of the alteration.

2.IPC Section 471: Using as genuine a forged document:

"Whoever fraudulently or dishonestly uses as genuine any document which he knows or has reason to believe to be a forged document, shall be punished in the same manner as if he had forged such document."

A. Provider NOT replying to legitimate query raised by insurer/ trust:

7. MISCONDUCT: The following acts of commission or omission on the part of a physician shall constitute professional misconduct rendering him/her liable for disciplinary action

7.7 Signing Professional Certificates, Reports and other Documents: Registered medical practitioners are in certain cases bound by law to give, or may from time to time be called upon or requested to give certificates, notification, reports and other documents of similar character signed by them in their professional capacity for subsequent use in the courts or for administrative purposes etc.

Chapter 1

1.3 Maintenance of medical records

1.3.1 Every physician shall maintain the medical records pertaining to his / her indoor patients for a period of 3 years from the date of commencement of the treatment in a standard proforma laid down by the Medical Council of India.

1.3.2. If any request is made for medical records either by the patients / authorised attendant or legal authorities involved, the same may be duly acknowledged and documents shall be issued within the period of 72 hours.

1.3.3 A Registered medical practitioner shall maintain a Register of Medical Certificates giving full details of certificates issued. When issuing a medical certificate he / she shall always enter the identification marks of the patient and keep a copy of the certificate. He / She shall not omit to record the signature and/or thumb mark, address and at least one identification mark of the patient on the medical certificates or report.

B. Provider employing non-MBBS RMOs/ DMOs:

1.6 Highest Quality Assurance in patient care: Physician shall not employ in connection with his professional practice any attendant who is neither registered nor enlisted under the Medical Acts in

force and shall not permit such persons to attend, treat or perform operations upon patients wherever professional discretion or skill is required.

C. Provider not complying with law of the land:

1.9 Evasion of Legal Restrictions: The physician shall observe the laws of the country in regulating the practice of medicine and shall also not assist others to evade such laws. He should be cooperative in observance and enforcement of sanitary laws and regulations in the interest of public health. A physician should observe the provisions of the State Acts like

- Drugs and Cosmetics Act, 1940; Pharmacy Act, 1948;
- Narcotic Drugs and Psychotropic substances Act, 1985;
- Medical Termination of Pregnancy Act, 1971;
- Transplantation of Human Organ Act, 1994;
- Mental Health Act, 1987;
- Pre-natal Sex Determination Test Act, 1994;
- Drugs and Magic Remedies (Objectionable Advertisement) Act, 1954;
- Bio-Medical Waste (Management and Handling) Rules, 1998 and such other Acts, Rules, Regulations made by the Central/State Governments or local Administrative Bodies or any other relevant Act relating to the protection and promotion of public health.

7.18 In the case of running of a nursing home by a physician and employing assistants to help him / her, the ultimate responsibility rests on the physician.

Vicarious responsibility

Liability exists in spite of the absence of blameworthy conduct on the part of the master

- Locum (replacement) doctor, although with his/ her own registration number
- Nurses and residents working directly UNDER registered doctor's supervision
- Any skilled OR non-skilled staff employed by registered doctor (unless it is proved that ALL possible care was taken to verify qualifications and other details)

7.19 A Physician shall not use touts or agents for procuring patients. ← PROs to get patients from remote areas.

7.20 A Physician shall not claim to be specialist unless he has a special qualification in that branch - treating patients that ideally should be treated by another specialty.

Not registering MLC/ FIR:

Relevant Sections/clause of Cr.P.C & IPC and code of ethics laid down by MCI, which state as follows:

- Section of 39 Cr.P.C: The attending doctor is duty bound to inform the police about the Medico Legal Case.
- Section 176 IPC: Omission to give notice or information to public servant by person legally bound to give it.
- Clause 1.9 - Evasion of Legal Restrictions from Code of Medical Ethics: The physician shall observe the laws of the country in regulating the practice of medicine and shall also not assist others to evade such laws.

7. Misconduct:

MCI APPENDIX –4

List of certificates, reports, notifications etc. Issued by doctors for the purposes of various acts / administrative requirements:

In connection with sick benefit insurance and friendly societies. (to be read together with 'Misconduct')

The following acts of commission or omission on the part of a physician shall constitute professional misconduct rendering him/her liable for disciplinary action

7.1 Violation of the Regulations: If he/she commits any violation of these Regulations.

7.8 A registered medical practitioner shall not contravene the provisions of the Drugs and Cosmetics Act and regulations made there under. Accordingly,

Prescribing steroids/ psychotropic drugs when there is no absolute medical indication in contravention of the above provisions shall constitute gross professional misconduct on the part of the physician."

Professional misconduct

The following acts of commission or omission on the part of a physician shall constitute professional misconduct rendering him/her liable for disciplinary action.

7.1 Violation of the Regulations: If he/she commits any violation of these Regulations.

7.2 If he/she does not maintain the medical records of his/her indoor patients for a period of three years as per regulation 1.3 and refuses to provide the same within 72 hours when the patient or his/her authorised representative makes a request for it as per the regulation 1.3.2.

7.3 If he/she does not display the registration number accorded to him/her by the State Medical Council or the Medical Council of India in his clinic, prescriptions and certificates etc. issued by him or violates the provisions of regulation 1.4.2.

Insurance Regulatory and Development Authority of India:
Sy No. 115/1, Financial District, Nanakramguda,Gachibowli,
Hyderabad – 500032

National Health Authority
7th & 9th Floor, Jeevan Bharati Building, Connaught Ln, Janpath,
Connaught Place, New Delhi, Delhi 110001