सत्यमेव जयते

Government of Mizoram

MIZORAM UNIVERSAL HEALTHCARE SCHEME (MUHCS)

Anti-Fraud Guidelines

Mizoram State Health Care Society

Department of Health & Family Welfare

2025

Contents

Abbreviations

CEO	Chief Executive Officer
CRC	Claims Review Committee
DVO	District Vigilance Officer
FIR	First Information Report
ICU	Intensive Care Unit
ISA	Implementing Support Agency
IT	Information Technology
LOS	Length of Stay
MMRC	Mortality and Morbidity Review Committee
OPD	Out Patient Department
MUHCS	Mizoram Universal HealthCare Scheme
MSHCS	Mizoram State Health Care Society
TPA	Third Party Administrator

Tables

1. Purpose and Scope

1.1 **Anti-Fraud Guidelines** for Mizoram Universal HealthCare Scheme (MUHCS) aimed at assisting the Government of Mizoram in designing and managing a robust anti-fraud system.

1.2 The scope of Anti-Fraud Guidelines covers prevention, detection and deterrence of different kinds of fraud that could occur at different stages of its implementation as can be elicited below:

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

Table 1: Scope of anti-fraud guidelines

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 Mizoram State Health Care Society (MSHCS) is the nodal agency for executing anti-fraud guidelines under MUHCS in the state of Mizoram.

2. Health Insurance Fraud under MUHCS

2.1 Principles

2.1.1 Any form of fraud under MUHCS is a violation of patients' right to health and misuse of publicresources.

2.1.2 MUHCS is governed based on a zero-tolerance approach to any kind of fraud and aims at detection, prevention and deterrence of fraudulent practices in 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 disclosinginformation as necessary in relation to fraud under MUHCS.

ii. ***Accountability*** shall mean clear functions, structures, systems and accountability forservices for effective management.

iii. ***Responsibility*** shall mean management conformity or compliance with soundorganizational principles for anti-fraud efforts under MUHCS.

iv. ***Independence*** shall mean a condition where MUHCS 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 arisingfrom agreements in anti-fraud efforts under MUHCS.

2.2 Definition of fraud under MUHCS

2.2.1 Fraud under MUHCS 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 himself / herself 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 as *fraud* shall be deemed to be *fraud* under MUHCS:

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

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

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.

[1] '**Errors**' are un-intentional 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 MUHCS, 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 MUHCS. Whereas **fraud** is willful anddeliberate, involves financial gain, is done under false pretense and is illegal, **abuse** generally fails to meet oneor 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 daycare procedure to overnight admission.

2.3 Types of fraud under MUHCS and who may conduct fraud

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

Fraud Type	Description
Beneficiary Fraud	Fraud conducted by an eligible beneficiary of MUHCS or an individual impersonating as a beneficiary.
Provider Fraud	Fraud conducted by any private or public health care provider empaneled for providing services under MUHCS.
Payer Fraud	Fraud conducted by an employee of MSHCS, or personnel employed by any of the agencies contracted by the MSHCS directly or indirectly involved with MUHCS. This could include but is not limited to Insurance Companies, Third Party Administrators, Implementing Support Agencies, IT solutions provider, and agencies responsible for management, monitoring or audit.

Table 2: Types of Fraud

3 Institutional Arrangements for Anti-Fraud Efforts

3.1 Dedicated Anti-Fraud Cell

3.1.1 **Mandate and functions**: The MSHCS 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 MUHCS.
b. Review and update the state anti-fraud framework and guidelines based on emerging trends for service utilisation and monitoring data.
c. Capacity building on anti-fraud measures under MUHCS including field verification and investigations.
d. Liaise with the IT team / agency to ensure that the IT platform is periodically updated withfraud triggers based on review of trends.
e. Liaise with the monitoring unit of the MSHCS for triangulating fraud related data analytics with the overall service utilisation trends emerging under MUHCS.
f. Provide evidence-based insights to the MSHCS on trends emerging from state-specific fraud data analytics.
g. Handle all fraud related complaints that MSHCS may receive and liaise with other units of MSHCS, especially the monitoring and audit units.
h. Take *Suo moto* action based on *prima facie* evidence as deemed appropriate.
i. Undertake fraud investigations as required, prepare investigation reports that can standlegal scrutiny if needed, file First Information Report (FIR) with the police as needed, navigate the legal system, pursue recovery and all other tasks related fraud investigation and follow up actions, including notice to treating doctors (if required), etc.
j. Incentivise internal team/outsourced agency involved in fraud management based onperformance (if applicable).
k. Publish data on utilization, claim rejection, suspension, de-empanelment, etc.

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

a. Be an independent unit in the MSHCS reporting directly to CEO, MSHCS.
b. Be headed by an Officer who reports directly to CEO, MSHCS.
c. Recommended staffing pattern for the Anti-Fraud Cell under the Insurance, Assurance, and mixed (both insurance and assurance) modes: (Table 3)

State level Anti-Fraud staff	Insurance Mode	Assurance and Mixed Mode
Head	1	1
Officer(s)	1	1
District & facility level staff		
District Vigilance Officer(s)	1 in each district	1 in each district

Table 3: State Anti-fraud Unit

d. To avoid possibilities of collusion, it is recommended that the District Vigilance Officers be directly recruited by the MSHCS.

Refer to *Annexure 3* for organogram of the Anti-Fraud Cell in the MSHCS and indicative terms of reference for various positions.

3.2 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

3.3 Leveraging existing health department structures to strengthen anti-fraud efforts

3.3.1 It is important to integrate and institutionalize anti-fraud efforts within the Department of Health & Family Welfare.

3.3.2 MSHCS may sought the feasibility to coordinate with existing governance and monitoring structures such as the District Health Societies, office of the Senior Chief Medical Officers or the District Medical Superintendents or their counterparts, structures at the block level and sub-divisional level such as CHC/PHC/SDH/UPHC.

3.3.3 Other medium of redressal mechanisms in force under the Government can be utilized for reporting unethical / fraudulent practices / behaviour.

3.4 Operations and management of the Anti-Fraud Cell at the State Level

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

3.4.2 **Annual action plan**: The Anti-Fraud Cell may propose an annual anti-fraud action plan which may include but not be limited to:

a. Statement detailing detected 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.

3.4.3 **Review of anti-fraud efforts**: Apart from review meetings conducted as and when required, the Anti- Fraud Cell shall ensure at least a quarterly structured anti-fraud meeting with the MSHCS management team. Alternately, anti-fraud efforts review could feature as a part of the ongoing review meetings of the MSHCS. 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.

4 Anti-Fraud Measures under MUHCS

4.1 Fraud prevention

4.1.1 **Referral protocols for benefits that are more prone to fraud and abuse**: Procedure or certain benefits under MUHCS that are more prone to fraud may either be reserved only for empaneled public providers or can be availed only on referral from a public provider. The existing portability procedures under MUHCS is to be followed, i.e., Medical Referral Board approval shall be mandatory for all portability cases.

4.1.2 **Ensure that all contracts signed by MSHCS with any party (Insurer, ISA, TPA, provider, IT agency, etc.) have adequate anti-fraud provisions that are enforceable:** The MSHCS should ensure that all model contracts of MSHCS 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 mentioned in the terms of the contract. The MSHCS should ensure that the contracts have adequate dis-incentives and penalties for abuse and fraud.

4.1.3 **Beneficiary identification / verification:** The MSHCS and its affiliates shall ensure strict compliance to MUHCS guidelines for beneficiary verification. For beneficiary fraud prevention, the Anti-Fraud Cell may audit records of pending and verified beneficiaries under Beneficiary Identification System.

4.2 Fraud detection

4.2.1 **Claims management**

a. The MSHCS shall ensure strict compliance to MUHCS guidelines for claims management.
b. Claim data analysis for early detection of fraud may be conducted 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 MSHCS from relevant government agencies.
d. In conducting claim data analysis, the Anti-Fraud Cell may coordinate with the medical audit team, claims processors and adjudicators in the TPA / ISA / MSHCS or the CRC / MMRC and other parties as necessary.

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

a. Data analysis comparing providers on such indices as utilization, performance, outcomes, referrals, de-empanelment, 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.

4.2.3 **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 MSHCS data systems be used to identify benefit utilization patterns that may assist in the case development and in the review.

4.2.4 **Routine reviews on problem areas:** As part of fraud and abuse detection strategy, the Anti-Fraud Cell may identify areas of focus that 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 MUHCS.
b. ensuring the authenticity of enrolled beneficiaries.
c. ensuring that provider employees understand MUHCS guidelines, can define fraud and know where, how, and when to report a fraud or potential fraud.

4.2.5 **Random reviews and beneficiary interviews:** MSHCS and its affiliates may plan for a minimum level of random reviews, in which a selected universe of beneficiaries is contacted for interviews. Medical records should also be reviewed to identify any possible errors or evidence of abuseand/or fraud. All such reviews shall be as per the guidelines issued by the MSHCS from time to time.

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

4.2.7 **Use of feedback and quality improvement:** The results of reviews (including feedback) and investigations should be used to improve MUHCS implementation systems. The goal is to prevent fraud and abuse from recurring. This use of feedback is integral to MUHCS quality improvement.

4.3 Guidelines for deterrence

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

4.3.2 To enable the MSHCS to take firm actions against fraud, MSHCS may consider stringent penalties and firm disciplinary actions.

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

4.3.4 The MSHCS may demand the providers to take firm action including issuing warnings and showcause notices to treating doctors found indulging in unethical practices.

4.4 Monitoring effectiveness of anti-fraud measures

4.4.1 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 Annexure 4. The MSHCS is at liberty to add more indicators as required.

4.4.2 The Anti-Fraud Cell may set up mechanisms of quarterly reporting against these indicators and recommend corrective measures to the CEO, MSHCS.

5 Use of IT in Anti-Fraud Efforts

5.1 Fraud triggers: The IT infrastructure should have a comprehensive automated fraud trigger alerts based on basic outlier analysis and rule-based analysis.A list of illustrative fraud triggers is provided in Annexure 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 MSHCS and the IT platform be constantly updated with new triggers as required.

5.2 Data mining and analytics: The IT infrastructure set up by the MSHCS is expected to have at least the basic fraud data analytics that allows for rule-based and outlier-based analysis. The MSHCS may engage an external agency for advanced analytics that may include predictive modelling regression techniques and use of social network analysis. 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.

5.3 Automated tools to assist in fraud management: The IT platform shall have automated security layers and tools to prevent fraud. Security within data processing systems, segregation of responsibilities to prevent conflict of interest and ensure internal checks and balances, passwords 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.

6 Managing Fraud Complaints

6.1 Fraud under MUHCS may either be detected internally by the Anti-Fraud Cell or may be externally reported. Sources of information and mechanism of reporting are highlighted below:

Internal Detection Sources	External Reporting
• Audit reports • Monitoring reports • Filed visit reports • Routine validation of provider data • Random reviews and beneficiary interviews • Unannounced site visits • Use of feedback • Data analytics dashboard	• From any individual or agency irrespective of their engagement with the beneficiaries. • In writing through email / letter to the MSHCS • On MUHCS helpline / call-centre. • On grievance redressal helplines, if any, set up under the Chief Minister's office. • Direct confrontation / information through other media.

6.2 MSHCS shall ensure that the identity of those filing grievances related to suspected fraud shall be kept confidential until the investigation is completed, and it is ascertained that fraud has been committed. 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 Executive Officer (CEO) of MSHCS. Other members of the investigation team may include members of the medical audit team, monitoring and evaluation team, district level staff as deemed appropriate by CEO, MSHCS. The CEO may, at his / her 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, verbal examination of concerned individuals, and submit a detailed investigation report to the CEO within 7 working days. The investigation report shall at the minimum include all details of the occurrence 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 MSHCS may issue a show-cause notice to the accused entity providing it within 7 working days to respond to the allegations and provide justification.

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.

7 Recoveries and Penalties Post Confirmation of Fraud

One or more of the following actions may be taken against the EHCP which has been found to commit fraud:

7.1 MSHCS may execute the following actions based on the severity of offence committed.

7.1.1 **Recovery of amount including penalties from EHCP:** Once it is confirmed that the EHCP has been indulging in fraudulent practices, recovery of excess amount paid for fraudulent claims to EHCP may be recovered by MSHCS. As recommended by MSHCS, SAA may levy additional penalties to the EHCP.

7.1.2 **Issuance of 'Show cause' to EHCP:** Based on the audit of the EHCP, if MSHCS believes that there is clear evidence of EHCP indulging in fraudulent practices.

7.1.3 **Suspension of EHCP:** For the EHCPs which have been issued show cause notice or if the MSHCS observes at any stage that it has data/ evidence that suggests that the EHCP is involved in any fraudulent practices, MSHCS may recommend for suspension of EHCP to relevant authority.

7.1.4 **De-empanelment of EHCP:** If the formal investigation conducted confirms that the EHCP is indeed indulging in fraudulent practices, MSHCS may recommend for de-empanelment of EHCP to relevant authority.

7.2 Action under Criminal Law: The criminal case (FIR) may be filed against the concerned under the relevant provisions of the applicable law.

7.3 No appeal or revision against the order of recovery may be entertained by the competent authority unless minimum 50% of the amount ordered to be recovered is deposited by the EHCP.

7.4 Legal and punitive action against the beneficiary using fraudulent means to get treatment (as defined in Annexure 1 – Types of Fraud)

7.4.1 Cancellation of MUHCS Card and blacklisting the beneficiary and the entire family.

7.4.2 Lodging a FIR with the local police authority

7.4.3 Collecting the entire treatment cost in cash

Annexure 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 MUHCS.
e. Engaging in a conspiracy with service providers to submit false claims.
f. Knowingly receiving prescribed medicines and/or medical devices for resale.

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 referral of beneficiaries.
d. Giving beneficiaries an inappropriate referral in order to gain a particular advantage.
e. Delays in scheduling treatment in anticipation of financial gain from beneficiaries or luring beneficiaries of preferential and early treatment in lieu of bribes.
f. Collecting unauthorized fees from beneficiaries.
g. Diagnosis / Package upcoding (change of diagnosis code and/or procedure to a code of higher rate) and procedure code substitution.
h. Cloning of claims from other patients (duplication of claims from other patients' claims).
i. Phantom visit (claim for patients' false visit).
j. Phantom procedures (claim for procedures never performed).
k. Phantom billing (claim for services never provided).
l. Services unbundling or fragmentation (claim for two or more diagnosis 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).
m. Duplicate/repeated billing (claim repeated for the same case).
n. Cancelled services (claim for services that are cancelled).
o. Measures of no medical value (claim for measures taken inconsistent with medical needs or indications).
p. Unnecessary treatment and/or medically inappropriate treatment.
q. Provision of counterfeit medicines.
r. Indulge in unethical practices not permissible under guidelines of 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.

Payer Fraud

a. Engaging in a conspiracy with health facilities to falsify information with the aim of meeting empanelment criteria/becoming empanelled under MUHCS.
b. Engaging in a conspiracy with beneficiaries and/or service providers to submit false claims.
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 acting against complaints of fraud received against provider(s).

Note: Reference to 'any of the agencies contracted by the MSHCS directly or indirectly involved with MUHCS' 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.

Annexure 2: Fraud Triggers

Claim History Triggers

a. Impersonation.
b. Mismatch of in-house document with submitted documents.
c. Second claim in the same year for an acute medical illness/surgical.
d. Claims from multiple hospitals with same owner.
e. Claims for hospitalization at a hospital already identified on a "watch" list or blacklisted hospital.
f. Claims from members with no claim free years, i.e., regular claim history.
g. Same beneficiary claimed in multiple places at the same time.
h. Excessive utilization by a specific member belonging to the beneficiary Family Unit.
i. Deliberate blocking of higher-priced package rates to claim higher amounts.
j. Claims with incomplete/ poor medical history: complaints/ presenting symptoms not mentioned, only line of treatment given, supporting documentation vague or insufficient.
k. Claims with missing information like post-operative histopathology reports, surgical / anaesthetist notes missing in surgical cases.
l. 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)
m. Multiple claims towards the end of policy cover period, close proximity of claims.

Admissions Specific Triggers

a. Members of the same beneficiary family getting admitted and discharged together.
b. High number of admissions.
c. Repeated admissions.
d. Repeated admissions of members of the same beneficiary family unit.
e. Admission beyond capacity of hospital.
f. Average admission is beyond bed capacity of the provider in a month.
g. Excessive ICU (Intensive Care Unit) admission.
h. High number of admissions at the end of the Policy Cover Period.
i. Claims for medical management admission for exactly 24 hours to cover OPD treatment, expensive investigations.
j. Claims with Length of Stay (LOS) which is in significant variance with the average LOS for aparticular ailment.

Diagnosis Specific Triggers

a. Diagnosis and treatment contradict each other.
b. Ailment and gender mismatch.
c. Ailment and age mismatch.
d. One-time procedure reported many times.
e. Treatment for which an Empanelled Health Care Provider is not equipped or empanelled for.
f. ICU/ Medical Treatment blocking done for more than 5 days of stay, other than in the case of critical illnesses.

Billing and Tariff based Triggers

a. High value claim from a small hospital/nursing home, not consistent with ailment and/or provider profile.

General

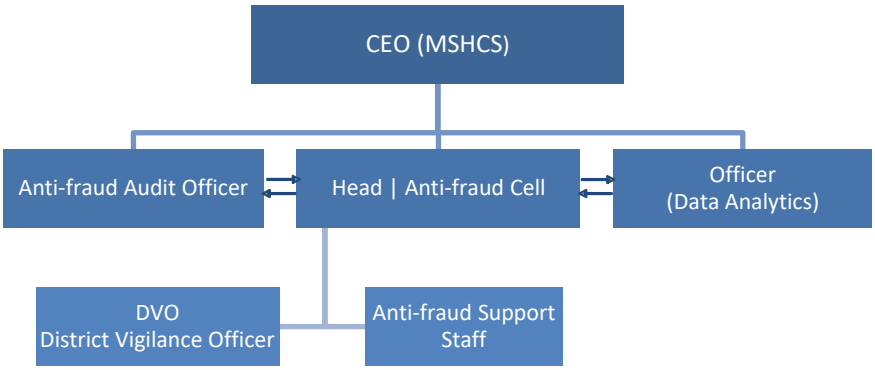
a. Qualification of practitioner doesn't match treatment.
b. Delayed information of claim details to the Insurer.

Annexure 3: Anti-Fraud Cell – Structure and Composition

At the Mizoram State Health Care Society (MSHCS)

For MSHCS, it is proposed to have a combined unit for Anti-fraud, medical audit and vigilance at the state level and to have Vigilance Officers at district level. The structure in MSHCS is proposed to remain same.

ORGANOGRAM OF THE ANTI-FRAUD CELL (MSHCS)



Recommended Positions, skills and key responsibilities:

State Level

Position	Education and skill set	Key responsibilities
Head – Anti fraud, vigilance and legal	- Medical Graduate (MBBS) - 5 years' experience, desirable. - 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 deterrent measures as per anti-fraud guidelines.	- To implement anti-fraud management guidelines laid down by MSHCS 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 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 deterrent measures, etc. as per guidelines against fraudsters

Data Analytics Officer	- Graduate - 5 years, preferably in MIS, reporting in volume business industry / health schemes. - Basic knowledge of Computer application equivalent to Course on Computer Concepts (CCC) of National Institute of Electronics and Information Technology (NIELIT) or Diploma in Computer Application / Certificate in Computer Application from institutions recognised by the Mizoram State Council of Technical Education (MSCTE). - 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 Officer	- Graduate. - 3 years, preferably investigation related field jobs. - Good communication skills, sharp and investigative mindset. - Knowledge of hospital billing practices desirable.	- To carry out field investigationof 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.
Anti-fraud support staff	- Graduate. - 5 years' experience in health claims processing/audit, desirable. - 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.

Annexure 4: Measuring Effectiveness of Anti-Fraud Efforts

1. Share of pre-authorization rejected
2. Share of pre-authorization and claims audited
3. Claim repudiation / denial / disallowance ratio
4. Reduction in number of enhancements requested per 100 claims
5. Number of providers de-empanelled
6. Instances of single disease dominating a geographical area are reduced
7. Disease utilization rates correlate more with the community incidence
8. Number of enquiries reports against hospitals
9. Number of enquiries reports against own staff
10. Number of FIRs filed
11. Incidence rate of detected fraud
12. Percent of pre-authorizations audited
13. Percent of post-payment claims audited
14. Fraudulent claims as a share of total claims processed
15. Number of staff removed or replaced due to confirmed fraud
16. Number of actions taken against confirmed fraudulent hospitals in a given time period
17. Amount recovered as a share of total claims paid
18. Share of red flag cases per 100 claims
19. Number of frauds reported on helplines
20. Movement of averages: claim size, length of stay, etc.