Anti-Money Laundering / Counter Financing Terrorism (AML / CFT) Policy

November 2022

Key Policy Information:

Policy reference number	Policy Owner	Policy Approver	Creation date
SHAIC – AMLCFT	Principal Officer	Board	20-03-2013

Summary - Version Control:

Version	Reviewed By	Approved By	Revision date	Reason for review
1	Chief Financial Officer	Board	2012-13/ March 20 2013	Initial Policy
2	Chief Financial Officer	Board	2018-19/ May 09 2018	Periodical Review
3	Chief Financial Officer	Board	2021-22/ February 14 2020	Periodical Review
4	Risk Management Committee	Board	2022-23/ November 09 2022	New AML Master Circular 2022

Table of Contents

1. Introduction

1.1 Background

The Prevention of Money Laundering Act, 2002 (PMLA), brought into force with effect from 1st July 2005, is applicable to all financial institutions. Giving reference of this Act, IRDAI had been issuing circulars on Anti Money Laundering/Counter – Financing of Terrorism (AML/CFT) and has released the master circular on 8th March 2013 and August 1, 2022 ("Master Circular"). In these circulars, IRDAI has included insurers in the category of Financial Institutions and has further mandated that each insurer (including standalone Health Insurer) should have an AML/CFT program ("Program").

Star Health and Allied Insurance Co. Ltd. (hereafter referred to as the "SHAIC" or "Company") is placed with statutory duty to make a disclosure to the authorized officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of drug trafficking or of a predicated offence, or was/is intended to be used in that connection, is passing through the institution. Such disclosures are protected by law, enabling the person with information to be able to disclose the same without any fear.

1.2 Objective

The objective of this policy is to manage and mitigate the risks arising from money laundering practices prevailing in the Health insurance sector by adhering to Master Circular on AML/CFT Guidelines for All Insurers (including standalone Health Insurer)

1.3 Applicability

SHAIC requires its employees, agents, intermediaries and corporate agents to adhere to all the applicable laws, rules and regulations generally in relation to AML/CFT norms and also the specific requirements mentioned in this Policy and all resulting standards, procedures, internal controls and guidelines. The Company has a zero tolerance for any violations to the requirements detailed in this Policy. In case of violations to this Policy, SHAIC reserves the right to take appropriate management measures (at its sole and absolute discretion) as defined in its employee and agents disciplinary action matrix/policies, including the termination of its business relationship with the concerned.

HODs have the primary responsibility for implementing this Policy within their function. Compliance has the responsibility of making all the filings with the IRDAI within the specified timelines. The Company has designated Principal Officer (PO) to oversee the compliance of this Policy.

1.4 Review and approval of the policy

AML / CFT Policy of the Company will be approved by the Board and reviewed annually. This should be reviewed periodically on the basis of risk exposure and suitable changes (if any) be effected based on experience and to comply with the extant Act / Rules / Regulations and other applicable norms. In case of any modifications to be carried out after the review, the same will be approved by the Managing Director/s and subsequently, the same will be put up to the Board for approval.

2. Key elements of the AML/CFT Program

This Program would serve the purpose of discharging the SHAIC's statutory responsibility including the detection and reporting of possible attempts of money laundering or financing of terrorism, and would include at a minimum:

- Know Your Customer (KYC) Guidelines
- Performing Due Diligence
- Watch List Screening / Implementation of Section 51A of UAPA
- Risk Assessment / Categorization
- Transactional Monitoring Program
- New Business Practices / Developments
- Central KYC Registration (CKYCR)
- Appointment of a Designated Director and Principal Compliance Officer
- Recruitment
- Training and Communication
- Other requirements of the Program & applicable guidelines

The Company shall undertake procedural checks to ensure that the Company has knowledge of all the customers and their sources of funds, basis which customers propose to purchase the policies. A strict application of these procedures and controls is essential for all relevant transactions of the Company.

2.1 Know Your Customer (KYC) Guidelines

Company shall make reasonable efforts to determine the true identity of all customers (new and existing) by doing proper Customer Due Diligence (CDD). Effective procedures to be put in place to obtain requisite details for proper identification of new and existing customers.

- SHAIC shall verify and document identity, address, and recent photograph (in case of individual customers) as part of compliance with KYC norms. A list of documents to be verified under KYC norms for individuals and others is given in **Annexure 1 (**which is illustrative). No further documentation is necessary for proof of residence where the document of identity submitted also gives the proof of residence.
- Where a client is a juridical person, SHAIC identity of the person purporting to act on behalf of such client is to be verified and documents in support of the legal status of such person is to be obtained to find out the proof of its name, existence, address of its registered office/main place of business, powers that regulate and bind the legal person to the Company shall take steps to identify the beneficial owner and take all reasonable measures to verify his/her identity to their satisfaction so as to establish the beneficial ownership. Systems/processes laid down to meet this requirement shall be based on risk perception of the entity (e.g. in case of a public limited company verification and identification of shareholders of that company is not called for). KYC documents collected towards the identity and address of the client shall be duly certified by an authorized person of the Company.

- SHAIC may perform KYC process by any of the following methods:

a) Aadhaar based KYC through Online Authentication subject to notification by the Government under section 11A of PMLA Or

b) Aadhaar based KYC through offline verification Or

c) Digital KYC as per PML Rules (refer definition Below) Or

d) Video Based Identification Process (VBIP) as consent based alternate method of establishing the customer's identity, for customer. The process of VBIP has been specified in Annexure 2. Or

e) By using „KYC identifier" allotted to the client by the CKYCR Or

f) By using Officially Valid documents **AND**

g) PAN/Form 60 (wherever applicable) and any other documents as may be required by SHAIC where section 11A of PMLA states that -

If any reporting entity performs Aadhar based authentication to verify the identity of its client or the beneficial owner it shall make the other valid modes of identification (as maybe notified by central government) also available to such client or the beneficial owner.

The use of modes of identification shall be a voluntary choice of every client or beneficial owner who is sought to be identified and no client or beneficial owner shall be denied services for not having an Aadhaar number.

- Under Individual Policies, those individuals who are not able to undergo Aadhaar Authentication due to any injury, illness or old age or otherwise, or they do not wish to go for Aadhaar Authentication, they may submit their Officially Valid Documents (OVDs) at the time of commencement of Account based relationship.
- Under Group Insurance, KYC of Master Policyholders / Juridical Person / Legal Entity and the respective Beneficial Owners (BO) shall be collected.
- SHAIC shall collect customer information from all relevant sources, including from agents/intermediaries.
- SHAIC shall make sure that the insurance premium should not be out of proportion to income/ asset.
- At any point of time, If SHAIC is no longer satisfied about the true identity and the transaction made by the customer, a Suspicious Transaction Report (STR) should be filed with Financial Intelligence Unit-India (FIU-IND) if it is satisfied that the transaction meets the criteria specified in sub clause (g) of clause (1) of Rule 2 of the PML Rules (Refer Definition of Suspicious Transaction below) and any guidelines / indicators issued by IRDAI or FIU-IND.
- Insurance premium paid by persons other than the person insured should be looked into to establish insurable interest.
- Adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF.

KYC for New Customers

In case of new contracts, KYC shall be done before the issuance of every new insurance contract. Client due diligence with valid KYC documents of the customer/ client shall be done at the time of commencement of account based relationship. SHAIC may rely on the identification and verification steps that the company has already undertaken in case of an existing customer, unless company has doubts about the veracity of the information with it. The validity of KYC documents procured earlier shall be as per SHAIC's Underwriting Guidelines.

KYC in case of non-face-to-face business

In case of non-face-to-face business, such as tele-calling and digital marketing, collection of documentation shall be done within 15 days of issuance of the Policy. The extent of verification in respect of non-face-to-face customers will depend on the risk profile of the product and that of the customer as per the SHAIC Underwriting Guidelines.

Knowing Existing Customer/Client

- The AML/ CFT requirements are applicable for all the existing customers/ clients. Hence, necessary Client due diligence with KYC (as per extant PML Rules) shall be carried out for the existing customers from time to time on the basis of adequacy of the data previously obtained.
- In case of non-availability of KYC of the existing clients as per the extant PML Rules, the same shall be collected within 2 years for low risk customers and within 1 year for other customers (including high risk customers).
- For continued operation of accounts of existing customers having insurance policy of not more than aggregate premium of Rs. 50,000/- in a financial year, PAN/Form 60 may be obtained by such date as may be notified by the Central Government.

Redaction or blackout of client's Aadhaar number

Where client submits it's Aadhaar number (electronic or physical), the first 8 digits of the Aadhaar Card shall be redacted or blacked out through appropriate means.

Reliance on third party KYC

For the purposes of KYC norms, while SHAIC are ultimately responsible for customer due diligence and undertaking enhanced due diligence measures, as applicable, SHAIC may rely on a KYC done by a third party subject to the following conditions:

1. The Company immediately obtains necessary information of customer due diligence carried out by the third party.
2. The Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
3. The Company is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the Act.
4. The third party is not based in a country or jurisdiction assessed as high risk.

Where SHAIC relies upon third party that is part of the same financial group, they should obtain KYC documents or the information of the client due diligence within 15 days.

2.2 Performing Due Diligence

Simplified Due Diligence (SDD)

- Simplified measures as provided under sub clause (d) of clause (1) of Rule 2 of PML Rules (refer definition of Officially Valid Document below) are to be applied by the SHAIC in case of individual policies, where the aggregate insurance premium is not more than Rs 10000/ - per annum.
- However, Simplified Client Due Diligence measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific high risk scenarios apply, based on the Risk Assessment/categorization policy of the SHAIC. Based on the robust risk assessment, SHAIC may apply Simplified Due Diligence measures only in respect of customers that are classified as 'low risk'.

- The Due Diligence Program including policies, controls and procedures, shall be approved by the senior management, to enable the SHAIC to manage and mitigate the risk that have been identified either by the company or through national risk assessment.

Enhanced Due Diligence (EDD)

- Enhanced Due Diligence as mentioned in Section 12AA of PML Act. shall be conducted for high risk categories of clients.
- The customers having high risk profile such as non-residents Indians, high net worth individuals, trusts, charities, NGOs, organizations receiving donations, companies having close family shareholding or beneficial ownership, firms with sleeping partners, Politically Exposed Persons (PEP) shall undergo detailed/ enhanced due diligence as well as higher verification and counterchecks as per the SHAIC's Underwriting Guidelines.
- Contracts with all high risk proposals (few illustrative above) shall be concluded post review and internal approval from a senior underwriting official in line with the SHAIC's Underwriting Guidelines.
- SHAIC is required to take reasonable measures to determine whether a customer or beneficial owner is a PEP. In particular, proposals of PEP require approval of senior management, not below Underwriting Head /Chief Risk Officer Level.
- Company, basis the on-going risk management procedures, shall identify and apply enhanced due diligence measures to PEPs, customers who are close relatives of PEPs. These measures shall also to be applied to insurance contracts of which a PEP is the ultimate beneficial owner
- SHAIC should examine, as far as reasonably possible, the background and purpose of all complex, unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, SHAIC should be required to conduct enhanced due diligence measures, consistent with the risks identified. Conducting enhanced due diligence shall not be limited to merely documenting income proofs. It would mean having measures and procedures which are more rigorous and robust than normal KYC.

SHAIC shall -

i. Verify the identity of the clients preferably using Aadhaar subject to the consent of customer or;
ii. Verify the client through other modes/ methods of KYC as specified in these guidelines.
iii. Examine the ownership and financial position, including client's source of funds commensurate with the assessed risk of customer and product profile.
iv. Application of additional measures like gathering information from publicly available sources or otherwise.
v. Review of the proposal/contract by a senior official of the company where the customer or the related person is a Politically Exposed Person (PEP)
vi. Reasonable measures to know the customer's source of funds commensurate with the assessed risk of customer and product profile
vii. The measures adopted by the company shall be such that they satisfy the competent authorities, if so required at a future date, that due diligence was in fact observed by the Company in compliance with the provisions of applicable law, based on the assessed risk involved in a transaction/contract.

Due diligence for FATF identified countries having deficiencies in their AML/CFT regime

- Conduct enhanced due diligence while taking insurance risk exposure to individuals/entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime as defined under the SHAIC's Underwriting Guidelines.
- Pay Special attention to business relationships and transactions, especially those which do not have apparent economic or visible lawful purpose. In all such cases, the background and purpose of such transactions will as far as possible, have to be examined and written findings have to be maintained for assisting competent authorities.
- Agents/intermediaries/ employees to be appropriately informed to ensure compliance with this stipulation.
- Go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations while using the FATF Public Statements, being circulated through the General Insurance Council.
- Take similar measures on countries considered as high risk from terrorist financing or money laundering perspective based on prior experiences, transaction history or other factors (e.g., legal considerations, or allegations of official corruption).

Ongoing Due Diligence

- Besides verification of customer's identity at the time of initial issuance of contract, Risk Assessment and ongoing due diligence should also be carried out (if so required) at times when additional/ subsequent remittances are made.
- Any change which is inconsistent with the normal and expected activity of the customer should be flagged, further ongoing due diligence to be carried out and action shall be taken, if required.

2.3 Watch List Screening / Implementation of Section 51A of UAPA

No insurance contract shall be entered into with a customer whose identity matches with any person in the sanction list or with banned entities and those reported to have links with banned entities or terrorist organizations**.** SHAIC shall periodically check MHA website for updated list of banned entities. An updated list of such persons and entities shall be available for screening with the Underwriting Team. More specifically,

- At the new business stage, the screening of new and prospective customers shall be carried out prior to the issuance of the policy by the Underwriting Team
- To ensure existing customers (policyholders, insured, and payors) and entities details are also scrubbed / screened against the new updated banned individuals and entities, Company shall (a) on an ongoing basis
- As a matter of precaution, adequate screening of all employees, vendors and agents, intermediaries shall be done while hiring or contracting them
- In case of any record found to be matching with any individual or entities that are suspected to be engaged in terrorism, the procedure for informing / seizing / freezing / unfreezing of the insurance policy/s are to be followed as prescribed under the section 51A of the UAPA
- "Freezing of insurance contracts" would require not-permitting any transaction (financial or otherwise), against the specific contract

Under watch-list screening process, Company shall maintain an updated list of designated individuals/entities in electronic form and shall run a check on the given parameters on a regular basis to verify whether designated individuals/ entities are holding any insurance policies with the Company. An updated list of individuals and entities which are subject to various sanction measures as approved by Security Council Committee established pursuant to UNSC 1267 can be accessed from the United Nations website at https://www.un.org/securitycouncil/content/unsc-consolidated-list

The salient aspects of the Implementation of Section 51A can be referred from AML Master Circular.

2.4 Risk Assessment / Categorization

SHAIC has to carry out Risk Assessment exercise periodically based on risk exposure to identify, assess, document and take effective measures to mitigate its ML and TF risk for clients/customers or geographic areas, products, services, nature and volume of transactions or delivery channels etc. While assessing the ML/TF risk, SHAIC is required to take cognizance of the overall sector specific and country specific vulnerabilities, if any, that the Government of India / IRDAI may share with SHAIC from time to time. Further, the internal risk assessment carried out by SHAIC should be commensurate to its size, geographical presence, complexity or activities/ structure etc.

- In the context of the very large base of insurance customers and the significant differences in the extent of risk posed by them, as part of the risk assessment, SHAIC shall at a minimum, classify the customer into high risk and low risk, based on the individual's profile and product profile, to decide upon the extent of due diligence.
- The documented risk assessment shall be updated from time to time. SHAIC shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. It shall be made available to competent authorities and law- enforcement agencies, as and when required.
- Basis the key elements of the Program as detailed above, the Company shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. Exceptions, if any, on the key elements towards Risk Assessment shall be discussed by the respective HODs with Chief Risk Officer (CRO) and shall be tabled at the relevant management meeting.

Risk Categorization

- Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients. business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.
- For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and source of wealth can be easily identified and transactions in whose policies by and large conform to the known profile may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society, government departments and government owned companies, regulators and statutory bodies. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Notwithstanding the above, in case of continuing policies, if the situation warrants, as for examples if the customer profile is inconsistent with this investment through top-ups, a re-look on customer profile is to be carried out.
- For the high risk profiles, like for customers who are non - residents, high net worth individuals, trusts, charities, NGO"s and organizations receiving donations, companies having close family shareholding or beneficial ownership, firms with

sleeping partners, politically exposed persons (PEPs), and those with dubious reputation as per available public information who need higher due diligence, KYC and underwriting procedures should ensure higher verification and counter checks.

2.5 Transactional Monitoring Program

- Regular monitoring of transactions is vital for ensuring effectiveness of the AML/CFT procedures. This is possible only if the SHAIC have an understanding of the normal activity of the client so that it can identify deviations in transactions/ activities.
- SHAIC shall pay special attention to all complex large transactions/ patterns which appear to have no economic purpose. The SHAIC may specify internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. The background including all documents/ office records/ memorandums/ clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to IRDAI/ FIU-IND/ other relevant Authorities, during audit, inspection or as and when required. These records are required to be maintained and preserved for a period of five years from the date of transaction between the client and SHAIC.
- The Principal Officer of the SHAIC shall monitor and ensure that Suspicious transactions shall be regularly reported to the Director, FIU- IND.
- Further, the dedicated compliance cell of SHAIC shall randomly examine a sample of transactions undertaken by clients to comment on their nature i.e. whether they are in nature of suspicious transactions or not.

Contracts with Politically Exposed Persons (PEPs)

- It is emphasized that proposals of Politically Exposed Persons (PEPs) in particular requires examination by senior management.
- SHAIC is directed to lay down appropriate on-going risk management procedures for identifying and applying enhanced due diligence measures on an on-going basis to PEPs and customers who are close relatives of PEPs. These measures are also to be applied to insurance contracts of which a PEP is the ultimate beneficial owner (s).
- If the on-going risk management procedures indicate that the customer or beneficial owner(s) is found to be PEP, or subsequently becomes a PEP, the senior management should be informed on this business relationship and apply enhanced due diligence measures on such relationship.

Verification at the time of Payout / Claim stage (Free-look cancellation /Claims)

- SHAIC should make no payments to third parties except as provided in the contract or in cases like payments to beneficiaries/ legal heirs/assignees in case of death benefits.
- Necessary due diligence should be carried out of the policyholders / beneficiaries/ legal heirs/ assignees before making the pay-outs.

AML/CFT checks on free-look cancellations: Free-look cancellations need particular attention, especially in those cases where the client/agent indulges in free-look cancellations on more than one occasion.

2.6 New Business Practices / Developments

- SHAIC shall pay special attention to money laundering threats that may arise from
  - Development of new products

- New business practices including new delivery mechanisms
- Use of new or developing technologies for both new and pre-existing products.

- Special attention should especially, be paid to the „non-face-to-face" business relationships brought into effect through these methods.
- SHAIC should lay down systems to prevent the misuse of money laundering framework. Safeguards will have to be built to manage typical risks associated in these methods like the following:
  - Ease of access to the facility;
  - Speed of electronic transactions;
  - Ease of making multiple fictitious applications without incurring extra cost or the risk of detection;
  - The extent of verification in respect of such „non face-to-face" customers will depend on the risk profile of the product and that of the customer.
  - SHAIC shall have in place procedures to manage specific increased risks associated with such relationships e.g. verification of details of the customer through on-site visits.

2.7 Central KYC Registration (CKYCR)

- Government of India has notified the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.
- Where a customer submits a "KYC identifier" for KYC, SHAIC shall retrieve the KYC records from CKYCR. In such case, the customer need not submit the KYC records unless there is a change in the KYC information required by SHAIC as per Rule 9(1C) of PML Rules which states that no banking company, financial institution or intermediary, as the case may be, shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.
- If the KYC identifier is not submitted by the client / customer, SHAIC shall search (with certain credentials) for the same on CKYCR portal and record the KYC identifier of the client/ customer, if available.
- If the KYC identifier is not submitted by the client/customer or not available in the CKYCR portal, SHAIC shall capture the KYC information in the prescribed KYC Template meant for „Individuals" or „Legal Entities", as the case may be.
- SHAIC shall file the electronic copy of the client's KYC records with CKYCR within 10 days after the commencement of account based relationship with a client/ Customer (both Individual/ Legal Entities).
- Once "KYC Identifier" is generated/ allotted by CKYCR, SHAIC shall ensure that the same is communicated immediately to the respective policyholder in a confidential manner, mentioning its advantage/ use to the individual/legal entity, as the case may be.

The following details need to be uploaded on CKYCR if Verification/Authentication is being done using Aadhaar:

1. For online Authentication,

a) The redacted Aadhaar Number (Last four digits)

b) Demographic details

c) The fact that Authentication was done

2. For offline Verification

a) KYC data

b) Redacted Aadhaar number (Last four digits)

- At the time of periodic updation, it is to be ensured that all existing KYC records of individual/legal entity customers are incrementally uploaded as per the extant CDD standards. SHAIC shall upload the updated KYC data pertaining to inforce /paid-up policies against which "KYC identifier" are yet to be allotted/generated by the CKYCR.
- SHAIC shall not use the KYC records of the client obtained from Central KYC Records registry for purposes other than verifying the identity or address of the client and should not transfer KYC records or any information contained therein to any third party unless authorised to do so by the client or IRDAI or by the Director(FIU-IND).

2.8 Appointment of a Designated Director and Principal Compliance Officer

Appointment of a Designated Director

The Company has designated the Managing Director as its Designated Director and has communicated his name to FIU-India.

The responsibility of the Designated Director will be to supervise Company's Program in view of the local regulatory requirements and ensure overall compliance with the obligations imposed under the Act and the PMLA Rules. The Management, in furtherance of responsibilities of the Designated Director, has the primary responsibility of:

- undertaking all actions as specified under the Master Circular and any subsequent amendments or clarifications thereof
- ensuring compliance with all relevant sections as specified under the FIU India's 'Guidance Note on Red Flag Indicators for the Insurance Sector, issued in February 2016 ("FIU-India Guidance Note") – Extract of the "FIU India Guidance Note". In case of inconsistency between the FIU Guidance Note and IRDAI Regulations / Guidelines / Circulars, the requirements emanating from IRDAI Regulations / Guidelines / Circulars shall prevail
- providing all assistance to the Central Government in order to implement the provisions of the Unlawful Activities (Prevention) Act, 1967, ("UAPA") as detailed in this Policy

Appointment of Principal Officer

The Company has designated the Chief Risk Officer as its Principal Officer and has communicated his name to both IRDAI and FIU-India. The Company has entrusted the Principal Officer with the following responsibilities and rights:

- Ensure that the Program is implemented effectively and that all the Company's employees / agents / intermediaries are in compliance with their obligations under the Program and are properly monitored.
- Ensure that employees and agents have appropriate resources and are well trained to address questions regarding the application of the Policy.
- The Principal Officer of the SHAIC shall monitor and ensure that Suspicious transactions shall be regularly reported to the Director, FIU- IND.
- Timely access to customer identification data as well as other KYC information and records.
- To act independently and report to the senior management of the Company.

- Ensure compliance with the obligations imposed under chapter IV of the Act and the PMLA Rules

2.9 Recruitment

- SHAIC shall have adequate screening mechanism as an integral part of their personnel recruitment/hiring process.
- As most part of the insurance business is through intermediaries /representative of SHAIC, the selection process of intermediaries/ representative of SHAIC should be monitored scrupulously in view of set AML/CFT measures.
- The Company shall monitor the selection process of agents, monitor the sales practices followed by them and ensure that if any unfair practice is reported, appropriate actions are taken after due investigation.

2.10 Training and Communication

- All staff engaged in sourcing/ processing of policies and any other customer transactions shall be given AML training on the background to money laundering and the need for identifying and reporting suspicious transactions to the Principal Officer.
- Ongoing training programme shall be adopted to cater the need of staff dealing with new customers and claims to handle issues arising from lack of customer education. In case of any need based training based on roles, training team to cater the requirement. This can be adopted through different means like training, e-learning module, presentation, circulars, emailers, advisories, education series, screensavers or other digital means.
- Communication of policies relating to prevention of ML and TF to all level of management and relevant staff that handle policyholder's information.

2.11 Other requirements of the Program & applicable guidelines

KYC for creation of E-Insurance account

- In case of existing Shell Insurance Accounts of Insurance policyholders with KYC compliance, no fresh KYC shall be necessary for opening an eIA account or issuance of a policy.
- SHAIC shall also provide option for e-signature / OTP authentication as directed by the IRDAI Clarifications on Guidelines on insurance e-commerce and electronic issuance of insurance policies dated 7-Sept-2017 (IRDA/ BRK/ CIR/ INSRE/ 211/ 09/ 2017)

3 Reporting

The AML/CFT program envisages submission of Reports on certain transactions to a Financial Intelligence Unit-India (FIU-IND) set up by the Government of India to track possible money laundering attempts and for further investigation an action. (Annexure 3)

Compliance Certificate - SHAIC shall submit annual compliance certificate as provided within 45 days of end of Financial Year.

4 Internal Control/ Audit

- Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the SHAIC, guideline and related issues shall be ensured.

- The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and adequately trained, well-versed in AML/CFT policies, guideline and related issues
- Internal Audit Department shall regularly verify and ensure compliance with policies, procedures and controls relating to money laundering & terrorist financing activities on the basis of overall risk assessment including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff, of their responsibilities in this regard.
- Upgrade questionnaire and system from time-to-time in accordance with the extant PMLA Rules
- A detailed report with specific comments on the robustness of the internal policies and processes in regard and constructive suggestions where necessary to strengthen the policy and implementation to this shall be submitted at least annually, as part of the internal audit schedule.
- Exception reporting under AML/CFT policy should be done to Audit Committee of Board

5 Maintenance of records

- The Company, its Designated Director, Principal Officer and employees shall maintain the information/records of types of transactions mentioned under Rule 3 and 4 of PMLA Rules as well as those relating to the verification of identity of clients for a period 5 years as mentioned in the Master Circular. The records referred to in the said Rule 3 shall also be maintained for a period of 5 years from the date of transaction. Records, pertaining to all other transactions for which the Company is required to maintain records under other applicable legislations/regulations/rules, shall be maintained for a period as provided in the said legislations/regulations/rules but not less than for a period of five years from the date of end of the business relationship with the customer.

- Records can be maintained in electronic form and/or physical form. In cases where services offered by a third party service providers are utilized,
  - SHAIC shall be satisfied about the capabilities, and that technology, systems and measures are in place to safeguard the privacy of the data maintained and to prevent unauthorized access, alteration, destruction, disclosure or dissemination of records and data.
  - The physical or electronic access to the premises, facilities, automatic data processing systems, data storage sites and facilities including back-up sites and facilities and to the electronic data communication network of the service provider is controlled, monitored and recorded.
  - The service provider has established standard transmission and encryption formats and non-repudiation safeguards for electronic communication of data.
  - It should also be ensured that the provisions under the relevant and extant data protection statutes are duly complied with.
- SHAIC should implement specific procedures for retaining internal records of transactions both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity. SHAIC should retain the records of those contracts, which have been settled by claim or cancelled, for a period of at least five years after that settlement.

- In situations, where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed. Wherever practicable, seller to seek and retain relevant identification documents for all such transactions and report such transactions of suspicious funds.
- In case of customer identification data obtained through the customer due diligence process, account files and business correspondence should be retained (physically or electronically) for at least five years after the business relationship is ended.

6 Consequence Management in case of non-compliance

- As per the Company's core principle on AML, Company employees / agents / intermediaries' other associates who act in breach with the Policy and who may expose the Company to AML related risks shall be dealt with seriously in accordance with the company disciplinary action process and the law
- In addition, the Company has undertaken the following steps to strengthen the level of control on the agents and corporate agents:
    - As part of the contracts with employees, agents and corporate agents, a clause is included making the adherence of the KYC norms mandatory. In addition, as part of its contracts with agents and corporate agents, the Company reserves the right to include specific processes and documents required for KYC norms adherence
    - When faced with a non-compliant agent or corporate agent, the Company shall take necessary action to secure compliance. Services of defaulting agents who expose the Company to AML/CFT related risks on multiple occasions should be terminated and the details reported to IRDAI for further action

7 Report an Issue

Any exceptions should be brought to the immediate attention of the Company's AML Principal Officer. If anyone is unsure whether a transaction is suspicious, more information should be obtained from the customer and report the same to the Principal Officer through aml@starhealth.in. When reporting a suspicious transaction, include the name, policy/ proposal number, description of transaction, reason for suspicion, amount, and parties involved.

8 Appendices

8.1 Definitions

8.1.1 "Act": means The Prevention of Money Laundering Act, 2002 (15 of 2003) as amended from time to time.

8.1.2 "Money Laundering:" Section 3 of the Act defines the "offence of money laundering" as under:

Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering."

As per the Master Circular, money laundering is "moving illegally acquired cash through financial systems so that it appears to be legally acquired".

There are three common stages of money laundering as detailed below which are resorted to by the launderers and insurance institutions may unwittingly get exposed to a potential criminal activity while undertaking normal business transactions:

- ***Placement*** – the physical disposal of cash proceeds derived from an illegal activity;
- ***Layering*** – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of money, subvert the audit trail and provide anonymity; and

- ***Integration*** – creating the impression of apparent legitimacy to criminally derived wealth

If the layering process has succeeded, integration schemes place the laundered proceeds back into economy in such a way that they re-enter the financial system appearing to be normal business funds. Financial institutions are therefore, placed with a statutory duty to make a disclosure to the authorized officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of drug trafficking or of a predicated offence, or was or is intended to be used in that connection is passing through such institution. Such disclosures are protected by law, enabling the person with information to be able to disclose the same without any fear. Insurance institutions likewise need not fear breaching their duty of confidentiality owed to customers.

8.1.3 "Aadhaar number", means an identification number issued to an individual under sub-section (3) of section 3 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act), and includes any alternative virtual identity generated under sub-section (4) of that section;

Subsection (3) of section 3 of Aadhaar Act:

On receipt of the demographic information and biometric information under sub-section (1), the Authority shall, after verifying the information, in such manner as may be specified by regulations, issue an Aadhaar number to such individual.

Subsection (4) of section 3 of Aadhaar Act:

The Aadhaar number issued to an individual under sub-section (3) shall be a twelve-digit identification number and any alternative virtual identity as an alternative to the actual Aadhaar number of an individual that shall be generated by the Authority in such manner as may be specified by regulations.

8.1.4 "Authentication" means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;

8.1.5 "Beneficial owner" shall mean "an individual who ultimately owns or controls a client of a reporting entity or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person.

8.1.6 "Central KYC Records Registry" (CKYCR) means a reporting entity, substantially owned and controlled by the Central Government, and authorised by that Government through a notification in the Official Gazette to receive, store, safeguard and retrieve the KYC records in digital form of a client as referred to in clause (ha) in such manner and to perform such other functions as may be required under these rules

8.1.7 "Client" means a person that engages in a financial transaction or activity with the Company and includes a person on whose behalf the person that engages in the transaction or activity is acting.

Explanation: For the purpose of this guideline, the term client includes a customer/ person (Natural or Juridical) who may be a proposer or policyholder or master policyholder or insured or beneficiaries or assignees, as the case may be.

8.1.8 "Client Due Diligence" (CDD)" means due diligence carried out on a client referred to in clause (ha) of sub-section (1) of section 2 of the Act.

8.1.9 "Designated Director" means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under Chapter IV of the Act and the Rules and includes—

(i) the Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,

(ii) the managing partner if the reporting entry is a partnership firm,

(iii) the proprietor if the reporting entity is a proprietorship concern,

(iv) the managing trustee if the reporting entity is a trust,

v) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and

(vi) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

Explanation.—For the purpose of this clause, the terms “Managing Director” and “Whole-time Director” shall have the meaning assigned to them in the Companies Act, 1956 (1 of 1956);]

8.1.10 “Digital KYC” means the capturing live photo of the client and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the reporting entity as per the provisions contained in the Act.

8.1.11 “KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

8.1.12 “KYC Records” means the records, including the electronic records, relied upon by a reporting entity in carrying out client due diligence as referred to in rule 9 of these rules.

8.1.13 “Offline verification” shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar Act.

8.1.14 “On-going Due Diligence” means regular monitoring of transactions to ensure that they are consistent with the customers" profile and source of funds.

8.1.15 "Officially valid document" means the passport, the driving licence, the Permanent Account Number (PAN) Card, the Voter’s Identity Card issued by [Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number or any other document as notified by the Central Government in consultation with the [Regulator], [Provided that where simplified measures are applied for verifying the identity of the clients the following documents shall be deemed to be officially valid documents:— (a) identity card with applicant’s Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions; (b) letter issued by a gazetted officer, with a duly attested photograph of the person.

Provided further that where simplified measures are applied for verifying the limited purpose of proof of address of the clients, where a prospective customer is unable to produce any proof of address, the following documents shall [also] be deemed to be 'officially valid document':

(a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, Water bill);

(b) property or Municipal tax receipt;

(c) bank account or Post Office savings bank account statement [or if the reporting entity is located in an International Financial Services Centre, statement of foreign bank];

(d) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

(e) letter of allotment of accommodation from employer issued by State or Central Government Departments or Public Sector Undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and licence agreements with such employers allotting official accommodation; and

Provided also that in case the officially valid document presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Provided also that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorised by them capturing the photograph, name, date of birth and address of a foreign national shall also be considered as officially valid document:

Provided also that where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as are issued by the Unique Identification Authority of India;

8.1.16 "Politically Exposed Persons (PEPs)" are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

8.1.17 "Principal Officer" means any officer designated by the Company with the responsibility of complying with the obligations set out and defined in the Act, PMLA Rules and the Master Circular. Can also be referred as AML Principal Officer.

8.1.18 "Suspicious Transaction" means a transaction referred to in clause (h), including an attempted transaction, whether or not made in cash, which to a person acting in good faith-

(a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

(b) appears to be made in circumstances of unusual or unjustified complexity; or

(c) appears to have no economic rationale or *bona fide* purpose; or

(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;]

[*Explanation.* - Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organisation or those who finance or are attempting to finance terrorism.

8.1.19 "Video Based Identification Process (VBIP)" means an alternative (optional)electronic process of Identification/ KYC in paperless form, carried out by the authorised person (person authorised by the SHAIC and specifically trained for face-to-face VBIP) by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer/beneficiary to obtain identification information including the

necessary KYC documents required for the purpose of client due diligence and to ascertain the veracity of the information furnished by the customer/ beneficiary.

8.1.20 Words and expressions used and not defined in these guidelines but defined in the Insurance Act, 1938 (4 of 1938), Insurance Regulatory and Development Authority Act, 1999 (41 of 1999), the PML Act, the PML Rules, the Aadhaar Act, Unlawful Activities (Prevention) Act, 1967 shall have the meanings respectively assigned to them in those Acts, Rules, Regulations, Guidelines issued under those Acts, as the case may be.

Annexures

Annexure 1:

List of Documents for KYC purposes

Where the Client is an individual

i. Passport
ii. PAN Card (Only as proof of identity), – Also a standalone mandatory KYC document
iii. Voter's Identity Card issued by Election Commission of India
iv. Driving License
v. Aadhaar number* (**s**ubject to notification under section 11A of PMLA allowing SHAIC to perform online authentication)/ Proof of possession of Aadhaar (if offline)
vi. Job card issued by NREGA duly signed by an officer of the State Government
vii. Letter issued by the Unique Identification Authority of India or National Population Register containing details of name, address and Aadhaar number.
viii. Current passport with details of permanent / present residential address (updated up to previous month) provided they are supported by official valid documents carrying photograph issued by regulated entity / government like debit card, credit card, kisan card etc.
ix. Current statement of bank account with details of permanent / present residential address (as downloaded) provided they are supported by official valid documents carrying photograph issued by regulated entity / government like debit card, credit card, kisan card etc.
x. Any other documents approved by the government from time to time in line with the CKYC enablement

* Where a customer submits Aadhaar for identification and wants to provide current address different from the address available in the Central Identities Data Repository, the customer may give a self- declaration to that **effect** to SHAIC.

1. Provided that <u>where simplified measures for due diligence are applied</u> for verifying the identity of the clients the following documents shall be deemed to be 'officially valid documents':
    a. Identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions
    b. Letter issued by a gazetted officer, with a duly attested photograph of the person

2. Provided further that where simplified measures for due diligence are applied for verifying the limited purpose of proof of address of the clients, where a prospective customer is unable to produce any proof of address, the following documents shall be deemed to be 'officially valid documents':
    a) Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

b) Property or Municipal tax receipt;
c) Bank account or Post Office savings account statement;
d) Pension or family pension payment orders (PPOs) issued to retired employees by Government Department or Public Sector Undertakings, if they contain the address;
e) Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and
f) Documents issued by Government departments of foreign jurisdiction and letter issued by Foreign Embassy or Mission in India.

Features	**Documents**
Insurance Contracts with companies	i. Certificate of incorporation ii. Memorandum & Articles of Association iii. Permanent Account Number of the company iv. Resolution of the Board of Directors and Power of Attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf v. One copy of officially valid document containing details of identity and address, one recent photograph and Permanent Account numbers or Form 60 of the managers, officers or employees , as the case may be, holding an attorney to transact on the company's behalf (or) CKYCR No. of the person holding the attorney.
Insurance Contracts with partnership firms	i. Registration certificate, if registered ii. Partnership deed iii. Permanent Account Number of the Partnership firm; and iv. One copy of officially valid document containing details of identity and address, one recent photograph and Permanent Account numbers or Form 60 of the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf; (or) CKYCR No. of the person holding the attorney.
Insurance Contracts with trusts & foundations	i. Registration Certificate ii. Trust Deed iii. Permanent Account Number or form 60 of the Trust; and iv. One copy of officially valid document containing details of identity and address, one recent photograph and Permanent Account numbers or Form 60 of the managers, officers or employees, as the case may be holding an attorney to transact on its behalf; (or) CKYCR No. of the person holding the attorney.
Insurance Contracts with Unincorporated association or a body of	i. Resolution of the managing body of such association or body of individuals; ii. Permanent Account Number or Form 60 of the unincorporated associations or a body of individuals; iii. Power of attorney granted to him to transact on its behalf; iv. One copy of officially valid document containing details of identity and address, one

individuals	recent photograph and Permanent Account numbers or Form 60 of the managers, officers or employees, as the case may be holding an attorney to transact on its behalf; (or) CKYCR No. of the person holding the attorney. v. Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.

Note-:

(i) No further documentation is necessary for proof of residence where the document of identity submitted also includes the proof of residence/address.

(ii) Where a customer submits Aadhaar for identification and wants to provide current address different from the address available in the Central Identities Data Repository, the customer may give a self- declaration to that effect to the Company.

(iii) Under Individual Policies, those individuals who are not able to undergo Aadhaar Authentication due to any injury, illness or old age or otherwise, or they do not wish to go for Aadhaar Authentication, they may submit their Officially Valid Documents (OVDs) at the time of commencement of Account based relationship.

(iv) In case of high risk customers, KYC and underwriting procedures should ensure higher verification and counter checks based on the underwriting requirement.

(v) Any other 'Officially valid document' that shall be notified by the Central Government, in consultation with the Regulator from time to time.

Annexure 2

Video Based Identification Process(VBIP)

Insurers may undertake live VBIP by developing an application which facilitates KYC process either online or face-to-face in-person verification through video. This may be used for establishment/continuation/ verification of an account based relationship or for any other services with an individual customer/beneficiary, as the case may be, after obtaining his/her informed consent and shall adhere to the following stipulations:

a) The Insurer/authorised person while performing the VBIP for KYC shall record clear live video of the customer/beneficiary present for identification and obtain the identification information in the form as below:

i) Aadhaar Authentication if voluntarily submitted by the Customer/ beneficiary, subject to notification by the government under Section 11 A of PMLA or

ii) Offline Verification of Aadhaar for identification, if voluntarily submitted by the Customer/beneficiary or

iii) Officially Valid Documents (As defined in rule 2(d) under PML Rules 2005) provided in the following manner –

1) As digitally signed document of the Officially Valid Documents, issued to the Digi Locker by the issuing authority or

2) As a clear photograph or scanned copy of the original Officially Valid Documents, through the eSign mechanism.

b) The insurer may also utilize this facility to verify PAN (wherever applicable). The insurer/authorised person shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digi locker. Use of printed copy of e-PAN is not valid for VBIP.

c) The insurer/authorised person shall ensure that the online video is clear and the customer/beneficiary along with the authorised person in the video shall be easily recognisable and shall not be covering their face in any manner.

d) Live location of the customer/beneficiary (Geotagging) shall be captured (both for online/ face-to-face VBIP) to ensure that customer/beneficiary is physically present in India.

e) The authorised person/ Insurer shall ensure that the photograph and other necessary details of the customer/beneficiary in the Aadhaar/ Officially Valid Documents/ PAN matches with the customer/beneficiary present for the VBIP.

f) The authorised person/ Insurer shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

g) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, if voluntarily submitted by the Customer/ beneficiary, it shall be ensured that the generation of XML file or QR code is recent and not older than 3 days from the date of carrying out VBIP.

h) All accounts opened or any service provided based on VBIP shall be activated only after being subject to proper verification by the insurer to ensure that the integrity of process is maintained and is beyond doubt.

i) Insurers shall ensure that the process is a seamless, real-time, secured, end- to-end encrypted audio-visual interaction with the customer/beneficiary and the quality of the communication is adequate to allow identification of the customer/ beneficiary beyond doubt. Insurers shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

j) To ensure security, robustness and end to end encryption, the insurers shall carry out software and security audit and validation of the VBIP application as per extant norms before rolling it out and thereafter from time to time.

k) The audio-visual interaction shall be triggered from the domain of the insurers itself, and not from third party service provider. The VBIP process shall be operated by the Insurer/authorized persons. The activity log along with the credentials of the official performing the VBIP shall be preserved.

l) Insurers shall ensure that the video recording bears the GPS coordinates, date (DD:MM:YY) and time stamp (HH:MM:SS) along with other necessary details, which shall be stored in a safe and secure manner as per PML Rules.

While exercising Online VBIP, the Insurer shall exercise extra caution and the additional necessary details viz. IP address etc. shall be preserved by the insurer to substantiate the evidence at the time of need.

m) Insurers are encouraged to take assistance of the latest available technology (including Artificial Intelligence (AI) and face matching technologies etc.) to strengthen and ensure the integrity of the process as well as the confidentiality of the information furnished by the customer/beneficiary. However, the responsibility of identification shall rest with the insurer.

n) Authorized person of the insurer shall facilitate face to face VBIP process only at the customer/beneficiary end.

However, the ultimate responsibility for client due diligence will be with the insurer.

o) Insurer shall maintain the details of the concerned Authorised person, who is facilitating the VBIP.

p) Insurers shall ensure to redact or blackout the Aadhaar number as per extant PML Rules.

q) Insurer will adhere to the IRDAI Cyber security guidelines as amended from time-to-time along with the necessary security features and standard as mentioned below:

- The Video KYC application and related APIs/Web Services shall undergo application security testing (both grey box and white box) through an CERT-In empanelled vendor and all reported vulnerabilities shall be mitigated before moving into production.
- The infrastructure components used for hosting Video KYC application shall undergo vulnerability assessment and secure configuration review through an CERT-In empanelled vendor and all reported vulnerabilities shall be mitigated before moving into production.
- There shall be an end-to-end encryption from the customer/beneficiary to the hosting point of the Video KYC application. The minimum encryption standards and key lengths like AES 256 for encryption should be used.
- If the Video KYC application and video recordings are located at a third party location and/or in Cloud, then the third party location and/or cloud hosting location shall be in India.

Annexure 3

Reporting Obligations

- SHAIC shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML Rules in terms of Rule 7 thereof.
- The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist insurers in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by Insurers which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The AML Principal Officer, where branches are not fully computerized, should make the suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.
- Illustrative list of Suspicious Transactions would be shared by IRDAI through Life/ General Insurance Council. Further, Red Flag Indicators issued by FIU-IND also be taken in account for Suspicious Transaction, wherever necessary.
- While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis- represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. SHAIC shall not put any restriction on operations in the accounts where an STR has been filed. SHAIC shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.
- Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

- SHAIC shall leverage the broadest number of data points / records available with them in implementing alert generation systems to assist in identifying and reporting suspicious activities.

SHAIC should not enter into arrangement with any unregulated entity which may have an effect of directly or indirectly impairing any reporting obligations.

8.2 List of applicable regulations

Date of issuance	Ref. No	Name of Legislation
16-10-2002	3222_GI_2002_ENG	IRDA (Manner of Receipt of Premium) Regulations, 2002
20-01-2003	-	Prevention of Money Laundering Act, 2002
27-05-2013	IRDA/SDD/GDL/CIR/104/05/2013	AML/CFT Guidelines
08-08-2013	IRDA/SDD/MISC/CIR/158/08/2013	AML/CFT Guidelines for insurer
29-05-2015	IRDA/INT/GDL/INSRE/111/05/ 2015	Guidelines on Insurance Repositories and electronic issuance of Insurance policies
16-03-2017	IRDA/INT/GDL/PSP/058/03/2017	Revision in Guidelines on Point of Sales Person – Non-Life and Health
07-09-2017	IRDA/ BRK/ CIR/ INSRE/ 211/ 09/ 2017	Clarifications on Guidelines on insurance e-commerce and electronic issuance
01-08-2022	IRDAI/IID/GDL/MISC/ 160 /08/2022	Master Guidelines on Anti-Money Laundering/ Counter Financing Terrorism (AML.CFT), 2022