Asia OneHealthcare Group Anti-Money Laundering, Countering Financing of Terrorism and Countering Proliferation Financing Policy (CP/Eth/05; v1.1)

CONTENTS

1. Introduction and Purpose
2. Scope
3. Definitions
4. General Description of Money Laundering, Terrorism Financing and Proliferation Financing
5. Policy Statement
6. Risk-Based Approach
7. Due Diligence
8. Suspicious Transactions and Escalation
9. Record Keeping and Retention of Records
10. Training and Communication
11. Responsibility for the Policy
12. Effective Date and Review

1. Introduction and Purpose

1.1 Money laundering is the process of introducing money, property or other assets derived from illegal or criminal activities into the legal financial and business system so that they appear to originate from a legitimate source. Terrorism financing and proliferation financing may involve the collection, movement, use or making available of funds, assets or economic resources for terrorism-related purposes or for the proliferation of weapons of mass destruction.

1.2 This Anti-Money Laundering, Countering Financing of Terrorism and Countering Proliferation Financing Policy ("**Policy**") sets out the general framework adopted by Asia OneHealthcare Bhd and its subsidiaries ("**Asia OneHealthcare**" or the "**Group**") to manage the risk of the Group's businesses being used as a conduit for money laundering, terrorism financing, proliferation financing or other financial crime activities.

1.3 The Group recognises that its core business is the provision of healthcare services and that in Malaysia, healthcare providers are not generally regulated as reporting institutions under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("**AMLA**"), unless a particular Group entity or business activity falls within the relevant reporting institution categories. This Policy is therefore intended to provide proportionate guidance to employees on identifying, managing and escalating suspicious transactions or red flags which may arise in the Group's business operations.

1.4 This Policy complements, and should be read together with, the Group Code of Conduct and Business Ethics, Group Anti-Bribery and Anti-Corruption Policy, Group

Whistleblowing Policy & Procedures, procurement policies, finance policies and other applicable internal policies and procedures.

2. Scope

2.1 This Policy applies to all directors, employees and officers of the Group, and to all hospitals, medical centres, clinics, business units and subsidiaries within the Group.

2.2 Where appropriate, the standards in this Policy may also apply to consultants, agents, contractors, suppliers, service providers and other third parties acting for or on behalf of the Group.

2.3 The requirements in this Policy are minimum standards. Where a Group entity operates in another jurisdiction, it shall comply with the applicable local AML/CFT/CPF laws and regulatory requirements. Where a Group entity undertakes any activity which is subject to additional AML/CFT/CPF laws, regulations or contractual requirements, the stricter requirement shall apply, subject to advice from Group Legal & Compliance where necessary.

3. Definitions

Term	Meaning
AML/CFT/CPF	Anti-Money Laundering, Countering Financing of Terrorism and Countering Proliferation Financing.
Business Unit	Any hospital, medical centre, clinic, subsidiary, department, function or business unit within the Group.
Business Unit Management	The Hospital Chief Executive Officer, head of business unit, head of department or person acting in a similar capacity.
Employee	All directors, employees and officers of companies within the Group, whether permanent, temporary or contract.
Group	Asia OneHealthcare Bhd and its subsidiaries.
Group Corporate Function	A corporate function within the Group, whether at Management Office or Corporate Office which is overseen by the relevant functional head, Chief Financial Officer or other designated management personnel.
Reporting Institution	A person or entity carrying out activities specified under AMLA and subject to the relevant AML/CFT/CPF obligations.
Suspicious Transaction	A transaction, attempted transaction, request, arrangement or conduct which gives rise to suspicion of money laundering, terrorism financing, proliferation financing, sanctions evasion or other unlawful activity.

4. General Description of Money Laundering, Terrorism Financing and Proliferation Financing

4.1 Money laundering generally involves proceeds of unlawful activities which are processed through transactions, concealment or other means so that they appear to have originated from a legitimate source. It commonly involves three stages:

(a) Placement – introducing illegal funds, often cash, into the financial or business system;
(b) Layering – creating layers of transactions to disguise the source, ownership or audit trail of the funds; and
(c) Integration – placing the laundered funds back into the economy so that they appear legitimate.

4.2 Terrorism financing generally refers to the raising, movement, provision or use of funds or assets, whether from legitimate or illegitimate sources, to support terrorist acts, terrorists or terrorist organisations.

4.3 Proliferation financing generally refers to the act of raising, moving or making available funds, assets or economic resources for the proliferation of weapons of mass destruction or related materials, including where such activities are connected with targeted financial sanctions.

5. Policy Statement

5.1 The Group prohibits all involvement in money laundering, terrorism financing, proliferation financing and other financial crime activities, whether directly or indirectly.

5.2 Employees must not knowingly assist, facilitate, conceal or participate in any transaction, arrangement or dealing involving suspicious funds, assets, parties or activities.

5.3 Employees must be alert to circumstances where the Group's businesses, services, facilities, accounts or transactions may be misused for money laundering, terrorism financing, proliferation financing or other unlawful purposes.

5.4 Any suspected activity or red flag must be escalated promptly in accordance with this Policy. Where a legal or regulatory reporting obligation applies, the relevant entity must comply with the applicable local AML/CFT/CPF law and regulatory requirements, including suspicious transaction reporting, where applicable.

6. Risk-Based Approach

6.1 The Group adopts a practical risk-based approach to managing AML/CFT/CPF risks. Each department should take reasonable steps to identify, assess and understand the AML/CFT/CPF risks relevant to its operations, having regard to the nature of the transaction, the counterparty, the country or geographical area involved and the payment method.

6.2 Risk control and mitigation measures should be proportionate to the risk identified. Enhanced measures should be applied where higher risks or red flags are identified.

6.3 Examples of higher-risk situations include:

(a) payments made by or to third parties that are not parties to the contract;
(b) requests for refunds to a different and unrelated person, entity, bank account or country;
(c) requests to issue inaccurate invoices, receipts or descriptions of services; and
(d) pressure to bypass normal approval or due diligence processes.

7. Due Diligence

7.1 Each department shall apply due diligence measures which are appropriate to the nature and risk of the transaction or relationship. For payment-related matters, including receipts, cash payments, refunds, third-party payments and bank account verification, the staff handling finance, billing or the relevant payment-processing function shall be primarily responsible for carrying out appropriate checks. Other departments are responsible for identifying and escalating red flags which come to their attention in the course of managing the relevant customer, patient or business partner relationship.

7.2 For ordinary patient transactions, standard patient registration, billing and payment controls will generally apply. Enhanced due diligence may be required where red flags are identified.

7.3 Due diligence measures may include, where appropriate:
(a) identifying the customer, patient, payer, supplier, counterparty or business partner;
(b) verifying the identity, registration details and bank account information of the relevant party;
(c) understanding the purpose and intended nature of the transaction;
(d) obtaining supporting documents or confirmation from the relevant party; and
(e) conducting reputational or other screening where relevant.

7.4 If the relevant party refuses to provide basic information reasonably required for due diligence, the matter must be escalated before the transaction proceeds.

8. Suspicious Transactions and Escalation

8.1 Employees must escalate any suspicious transaction or red flag promptly. Employees should not ignore the concern or inform the relevant party that a suspicious matter is being reviewed or escalated. Employees must not warn or alert any external party, including any patient, payor, customer, vendor, supplier, agent or business partner that a suspicious matter has been identified or may be reported to any authority.

8.2 Examples of red flags include:

(a) refusal to provide information on identity or source of funds where transaction involves unusually large amounts of cash
(b) transactions that appear inconsistent with the party's business or profession;
(c) attempts to split or manipulate transactions to avoid internal thresholds or controls; and
(d) requests to create false or misleading invoices or receipts.

8.3 Where an employee identifies a red flag, the employee must report the concern to his or her Head of Department. The Head of Department shall escalate the matter to Group Finance and Group Legal & Compliance for assessment. Where the matter involves significant risk, Senior Management shall be informed as appropriate.

8.4 For purposes of this Policy, Senior Management may include the Group Chief Executive Officer, Group Chief Financial Officer, relevant Regional Chief Executive Officer or Regional Chief Operating Officer, Group General Counsel and Group Head of Internal Audit where relevant.

8.5 Group Finance, together with Group Legal & Compliance and relevant management, shall evaluate the grounds for suspicion and determine the appropriate next steps. Where required by law, a suspicious transaction report shall be made to Bank Negara Malaysia or the relevant authority in the applicable jurisdiction through a designated official of the Group.

9. Record Keeping and Retention of Records

9.1 Relevant records relating to transactions, due diligence, approvals, escalations and decisions must be retained in accordance with applicable law and the Group's record retention requirements by the respective Business Units and Group Corporate Functions.

9.2 Records may include, where applicable:

(a) documents relating to the identification of the customer, patient, payer, vendor, supplier, counterparty or business partner;

(b) documents relating to beneficial ownership, authority, bank account details or source of funds;
(c) contracts, invoices, receipts, payment approvals and transaction records;
(d) business correspondence and supporting documents;
(e) internal escalation records, assessment notes and decision records; and
(f) any other document required by law, regulation, internal policy or the relevant authority.

9.3 Records shall be retained for at least seven (7) years, unless a longer retention period is required by law, internal policy or other legitimate business requirement.

10. Training and Communication

10.1 The Group may provide training and awareness sessions to employees, particularly employees involved in finance, billing, patient services, procurement and business development roles.

10.2 Training and communications may cover AML/CFT/CPF risks, red flags, due diligence, escalation procedures and record keeping requirements.

11. Responsibility for the Policy

11.1 This Policy is reviewed and approved by the Board of Directors or where delegated by the Board, a relevant board committee. The Board sets the tone from the top and provides leadership and support for the Group's commitment to prevent money laundering, terrorism financing, proliferation financing and other financial crime risks.

11.2 The Audit Committee monitors the implementation and effectiveness of this Policy. Group Internal Audit may conduct periodic reviews to assess the effectiveness of relevant controls, and any significant audit findings and corrective actions may be reported to the Audit Committee or Board, where appropriate.

11.3 The respective Business Unit Management and Group Corporate Functions are responsible for implementation of this Policy and escalation of concerns via internal procedures and programmes.

11.4 Group Legal & Compliance is responsible for providing guidance on this Policy, supporting the review of escalated concerns and advising on legal or regulatory implications. Group Legal & Compliance and Group Finance shall jointly coordinate any required reporting to authorities, where applicable.

12. Effective Date and Review

12.1 This Policy shall be reviewed at least once every three (3) years, or earlier where required due to changes in law or internal governance requirements.