FORTICARE
HEALTH SYSTEMS INTERNATIONAL. INC.

ANTI-MONEY LAUDERING/COUNTER TERRORISM FINANCING (AML/CTF) POLICY MANUAL

Corporate Center
5F Dy International Building 1011 Gen Malvar St
Corner San Marcelino St Malate Manila Philippines

Trunkline: (02) 53142273
Mobile Number: (0927)2230304
Email Address: dpo.forticare@gmail.com
Website: www.forticareph.com

Data Privacy Monitoring and Compliance Division (DPMCD)	
Authored By	Mark Anthony Junio, Data Protection & Compliance Officer
Updated & Edited Date	August 25, 2024
Approved By / Date	

1. Introduction

1.1. Policy Statement

FORTICARE HEALTH SYSTEMS INTERNATIONAL INC. (Company) commits to sound financial stewardship of its assets and to fight any attempt to use its business to launder illicit money, including financing terrorist activities. It recognizes its obligation to join the government and other financial watchdogs, here and abroad, to restrict avenues for money laundering and terrorist financing.

To this end, the Company shall:

A. Verify to a reasonable level of certainty the identities of all new and existing clients.
B. Adopt a risk-based approach in the monitoring of client tax and accounting affairs.
C. Report any suspicious activity and record all anti-money laundering activities.
D. Maintain a sound record-keeping management system.

For this purpose, the Data Privacy Monitoring and Compliance Division (DPMCD) shall monitor and ensure the Company and each of its department's compliance with:

A. this Manual,
B. the Republic Act No. 9160, otherwise known as the Anti-Money Laundering Act of the Philippines and its Implementing Rules and Regulations,
C. Other relevant and applicable law,
D. Issuances of the Anti-Money Laundering Council, the Securities and Exchange Commission, and the Insurance Commission,
E. All other rules and regulations as hereinafter may be issued by appropriate regulatory bodies, and
F. Well-recognized international best practices that are applicable to the Company.

1.2. Policy Owner

Data Privacy Monitoring and Compliance Division (DPMCD)

1.3. Approval Authority

Any changes to this policy must be approved by the Board of Directors ("BOD") and as recommended by the Risk Management Committee.

1.4. Policy Review

This policy will be subject to periodic review at a maximum of one (1) year. In the event of any changes in regulations, country operations, nature of the business, or any events which will significantly impact the Company, this policy will be reviewed, updated immediately, and communicated to relevant employees.

2. Scope

This Policy applies to all employees and officers of Forticare Health Systems International Inc, and its affiliated companies.

3. Definition of Terms

For purposes of this manual, the following terms are hereby defined as follows:

A. **"Anti-Money Laundering Act" (AMLA)** refers to Republic Act No. 9160, as amended by Republic Act Nos. 9194, 10167, and 10365.

B. **"Anti-Money Laundering Council" (AMLC)** refers to the financial intelligence unit of the Republic of the Philippines which is the government agency tasked to implement the AMLA and The Terrorism Financing Prevention and Suppression Act (TFPSA).

C. "**Supervising Authority"** refers to the Bangko Sentral ng Pilipinas (BSP), the Securities and Exchange Commission (SEC), the Insurance Commission (IC), or the relevant regulatory bodies of the Designated Non-Financial Businesses and Professions.

D. **"Person"** refers to any natural or juridical person.

E. **"Covered Persons"** refers to the following:
- ❖ Person supervised or regulated by the BSP;
- ❖ Person supervised or regulated by the SEC;
- ❖ Persons supervised or regulated by the IC, such as:
    a. Insurance companies;
    b. Pre-need companies;
    c. Insurance agents;
    d. Insurance brokers;
    e. Professional reinsurers;
    f. Reinsurance brokers;
    g. Holding companies;
    h. Holding company systems;
    i. Mutual benefit associations; and
    j. All other persons and their subsidiaries and affiliates supervised or regulated by the IC.

F. **"Transaction"** refers to any act establishing any right or obligation, or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a covered person.

G. **"Covered transaction"** refers to a transaction in cash or other equivalent monetary instrument exceeding Five Hundred Thousand pesos (Php500,000.00)

H. **"Suspicious Transaction"** refers to a transaction, regardless of amount, where any of the following circumstances exists:

1. there is no underlying legal or trade obligation, purpose, or economic justification;
2. the client is not properly identified;
3. the amount involved is not commensurate with the business or financial capacity of the client;
4. taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA;
5. any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered person;
6. the transaction is in any way related to an unlawful activity or any money laundering activity or offense that is about to be committed, is being or has been committed; or
7. any transaction that is similar, analogous, or identical to any of the foregoing.

I. **"Client/Customer"** refers to any person who keeps an account or otherwise transacts business with a covered person. It includes the following:

1. Beneficial owner, or any natural person who ultimately owns a customer and/or on whose behalf is maintained or is conducted;
2. Transactor, agents, and other authorized representatives of beneficial owners;
3. Beneficiaries;
4. A company or person whose assets are managed by an asset manager;
5. Trustors/grantors/settlers of a trust; and
6. Insurance policyholder/owner, insured, pre-need plan holder, HMO client, or HMO enrolled member, whether actual or prospective.

J. "**Politically Exposed Person" (PEP)** refers to an individual who is or has been entrusted with a prominent public position in (a) the Philippines with substantial authority over policy, operations, or the use or allocation of government-owned resources; (b) a foreign State; or (c) an international organization.

K. **"Immediate Family Member of PEP"** refers to individuals related to the PEP within the second degree of consanguinity or affinity.

L. **"Close Relationship/Associates of PEPs"** refer to persons who are widely and publicly known, socially or professionally, to maintain a particularly close relationship with the PEP, and include persons who can conduct substantial domestic and international financial transactions on behalf of the PEP.

M. **"Beneficial Owner"** refers to any natural person who:

1. Ultimately owns or controls the customer and/or on whose behalf a transaction or activity is being conducted; or
2. Has ultimate effective control over a legal person or arrange;
3. Owns, at least, twenty percent (20%) shares, contributions, or equity interest in a juridical person or legal arrangement.

N. **"Identification Document"** refers to any of the following identification documents:

1. For Filipino citizens: Those issued by any of the following official authorities:
    - 1.1 Phil ID.
    - 1.2 Other identification documents issued by the Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;
    - 1.3 Other identification documents that can be verified using reliable, independent source documents, data, or information.
2. For foreign nationals:
    - 2.1 Phil ID, for resident aliens;
    - 2.2 Passport;
    - 2.3 Alien Certificate of Registration; and
    - 2.4 Other identification documents issued by the Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities.
3. For Filipino students:
    - 3.1 Phil ID
    - 3.2 School ID signed by the school principal or head of the educational institution;
    - 3.3 Birth Certificate issued by the Philippine Statistics Authority; and
4. For low-risk customers: Any document or information reduced in writing which the covered person deems sufficient to establish the client's identity.

O. **"Proceeds"** refers to an amount derived or realized from any unlawful activity.

P. **"Offender"** refers to any person who commits a money laundering offense.

Q. **"Unlawful Activity"** refers to any act or omission, or series or combination thereof, involving or having direct relation, to the following and more:

1. Terrorism and financing thereof
2. Trafficking- drugs, arms, human
3. Tax evasion, Smuggling
4. Bribery, Extortion, Blackmail
5. Kidnapping, Carnapping
6. Mail fraud, Counterfeiting
7. Robbery
8. Graft and Corruption, Plunder

4. Description of Money Laundering

Money laundering means the ways in which criminals change "dirty" money and other assets into "clean" money or assets that have no obvious links to their criminal origin.

The three basic stages of money laundering are:

1. **Placement**. During placement, "dirty" money derived from criminal activities is placed in the financial system.
2. **Layering**. To conceal the illegal origin of the placed funds and thereby make them more useful to criminals, the funds must be moved, dispersed, and disguised. Layering is the process of disguising the source of the funds through layers of financial transactions.

3. **Integration**. Once the funds are layered and can no longer be traced back to their criminal origins, they are integrated into the financial system and now appear "clean" and available for use by criminals. If layering has been successful, integration places the laundered money back into the economy and financial system in such a way that they appear as clean and legitimate.

Terrorist financing involves dealing with money or property that may be used for financing terrorist activities. The funds and property may be from either legitimate or criminal sources. They may be small amounts.

The methods used by terrorists to move money are substantially the same as those used by other criminals, such as the following:

1. **Traditional financial institutions:** Financial institutions are vulnerable to abuse by terrorists. Despite doing all that is required with respect to Customer Due Diligence, transactions related to the financing of terrorism may fail to set off any alarms or "red flags." For example, accounts can be opened, and small withdrawals and deposits which are less than any legal reporting requirements can be made.
2. **Alternative remittance systems:** Unregulated remittance systems such as hawala and hundi. These systems often have traditional roots or ethnic ties and operate in places where the formal financial sector is less established; funds can be transferred without any documentation.
3. **Cash couriers:** Cash is smuggled across borders, for example through land crossings and sea shipments where borders are uncontrolled.
4. **False invoicing:** False trade invoicing provides a means to transfer money between jurisdictions by overstating the value of the goods or services for which payment is due.
5. **High-value commodities:** Commodities like gold and diamonds can also be used to transfer value across borders as both are easy to convert into cash.

5. Known Your Client (KYC)

The Company has established a **Know-Your-Client (KYC)** Policy to ensure the identities of all new and existing clients are verified to a reasonable level of certainty. This will include all directors and shareholders with a stake holding of 20% or more of client companies, all partners of client partnerships, and every board member of client charities.

Moreover, the KYC policy encapsulates the Customer Acceptance Program of the Company. Sufficient Customer Due Diligence Form (CDDF) must be done prior to establishing a business relationship. Also, Forticare can terminate this relationship if in case the client is unable to comply with relevant CDDF measures, as required under the Anti-Money Laundering Act, as amended and relevant issuances, due to the fault of the client. More details can be found in Section 5.3 of the KYC Policy.

In accordance with the Forticare' Know-Your-Client Policy, the following are the minimum customer identification documents in which Forticare must collect from its corporate clients.

Customer Information	Identification Documents
✓ Name of the entity; ✓ Name of the authorized signatory; ✓ Name of the beneficial owner, if applicable; ✓ Official address;	✓ Certificates of Registration issued by the Department of Trade and Industry (DTI) for sole proprietors, or Certificate of Incorporation issued by the Securities and Exchange Commission (SEC) for

✓ Contact number or information; ✓ Nature of business; ✓ Specimen signatures or biometrics of the authorized signatory.	corporations and partnerships, and by the BSP for money changers/foreign exchange dealers and remittance agents; ✓ Secondary License or Certificate of Authority issued by the Supervising Authority or other government agency; ✓ Articles of Incorporation/Partnership; ✓ Latest General Information Sheet; ✓ Corporate/Partners' Secretary Certificate citing the pertinent portion of the Board or Partners' Resolution authorizing the signatory to sign on behalf of the entity.

**Refer to KYC Policy, Section 5.2.3 Minimum Customer Information, and Identification Documents*

To have a better understanding of the requirement, below are the minimum non-negotiable documentation titles incorporated in the Account Information Form in **Appendix A.**

PARTNERSHIPS	CORPORATIONS	OTHERS (e.g. Associations/Cooperatives)
✓ SEC/ DTI Certificate of Registration. ✓ Partner's Agreement/Resolution. ✓ List of Partners/Principal Stockholders	✓ SEC Certificate of Registration. ✓ Articles of Incorporation (Amended, if any). ✓ General Information Sheet (latest). ✓ Secretary's Certificate	✓ Certificate of Registration with appropriate government agencies. ✓ Articles of Association or Constitution. ✓ List of Directors and Key Officers

6. Risk Management

6.1 Risk Assessment

The business takes a risk-based approach to monitor the financial activities of its clients. Where appropriate, business owners should conduct preliminary due diligence before contracting with clients. This due diligence can be conducted with the assistance of DPMCD.

Due diligence requirements may vary depending on the result of the risk assessment. For the risk categorization and requirements, please refer to the **Know-Your-Client Policy, Appendix A, Risk Categorization**.

The business will actively not accept high-risk clients that are identified as follows:

a. Clients with businesses that handle unusually large transactions.
b. Clients with larger one-off transactions, or several transactions carried out by the same customer within a short space of time.
c. Clients with complex business ownership structures with the potential to conceal underlying beneficiaries.
d. Clients based in or conducting business in or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime, or drug production/distribution such as those in North Korea and Myanmar.
e. Situations where the source of funds cannot be easily verified.

f. Unusual patterns of transactions that have no apparent economic or visible lawful purpose.
g. Money sent to or received from areas known to have high levels of criminality or terrorist activity.

The business will conduct ongoing monitoring of business relationships with customers, to ensure that the documents, data, or information held evidencing the customer's identity are kept up to date.

The following are examples of changes in a client's situation that may be considered suspicious:

a. Transactions with no clear economic or legal purpose.
b. Payments to accounts where there is no connection to the relevant parties.
c. Payments across jurisdictions which is not connected to the underlying transaction.
d. Unusually complex transactions for no logical reason.
e. Loss-making transactions with no clear explanation.
f. Payments to tax-havens.

Whenever there is cause for suspicion, the client will be asked to identify and verify the source or destination of the transactions, whether they be individuals or company beneficial owners.

*No action needs to be taken if there is no cause for suspicion.

6.2 Compliance monitoring

The DPMCD will regularly monitor the following procedures to ensure they are being carried out in accordance with the AML policies and procedures of the business:

a. client identity verification;
b. reporting covered and suspicious transactions;
c. record-keeping.

The DPMCD will also monitor any developments in the Anti-Money Laundering Act and the requirements of the AMLC. Changes will be made to these policies and procedures of the business when appropriate to ensure compliance.

6.3 Reporting of Suspicious Activity

A Suspicious Transaction Report (STR) will be made to the AMLC as soon as the knowledge or suspicion that criminal proceeds exist arises. The DPMCD will be responsible for deciding whether the suspicion of illegal activity is great enough to justify the submission of an STR. See **Appendix B** for indicators of these transactions. Incidents of suspicious activity should be reported immediately to your Manager/Supervisor and concurrently logged in the Incident Reporting tracker.

6.4 Reporting of Covered Transactions

The Company shall report to the AMLC all covered transactions within five (5) working days from the occurrence thereof, unless the AMLC or any other equivalent Supervising Authority concerned prescribes a longer period not exceeding ten (10) working days.

6.5 Record-keeping

All records of all transactions shall be maintained and safely stored for five (5) years from the dates of transactions. With respect to closed accounts, the records on customer identification and transaction, account files, and business correspondence, shall be preserved and safely stored for at least five (5) years from the dates when they were closed.

Copies of any STR, together with any supporting documentation filed will be maintained for 5 years from the date of filing the STR. All records will be handled in confidence, stored securely, and will be capable of being retrieved without undue delay.

7. Training

All employees and officers shall always be trained on their responsibilities in relation to money laundering legislation to ensure awareness of how to identify and deal with transactions that may involve money laundering. A mandatory annual training shall be required from all employees.

8. Your Role as Stewards of the Company

Collect and understand documentation about prospective customers, agents, and business partners to ensure that they are involved in legitimate business activities and that their funds come from legitimate sources.

Follow your business rules concerning acceptable forms of payment. Learn the types of payments that have become associated with money laundering (for example, payments on behalf of a client from an unknown person). Follow your business Know-Your-Client procedures and rules on collecting and verifying information from our clients and related parties. In case a suspicious report will be filed with our AMLC or enhanced due diligence is to be done, you should not tip off the client by:

- Changing the way we handle the client;
- Informing other people not related to the investigation of the suspicions;
- Directly alerting the client of a suspicion

If you become aware of any suspicious payment transactions/requests, escalate the matter to DPMCD only:

- **Mark Anthony C. Junio**
  Data Protection & Compliance Officer
  Contact Number: (02)53142273, (0927)2230304
  Email Address: dpo.forticare@gmail.com

If there are transactions that are being proposed with parties in certain sanctioned countries (being countries which are the subject of economic or other sanctions imposed by the United States of America or the European Union, such transactions are not to proceed unless prior written approval from DPMCD is obtained.

Restricted Countries include:

a. North Korea
b. Myanmar
c. Any other country as may be provided hereinafter by DPMCD

In certain instances, the sale of certain goods/equipment (including software and technology) may be subject to export control regulations. This is because such goods/equipment may have dual-use (in addition to medical/civilian/commercial usage) which may threaten another country's security. If there is a contemplated sale of such goods/equipment, consult first with DPMCD. In case of doubt, always refer the matter to DPMCD. In case of doubt, always refer the matter to DPMCD.

9. Policy Compliance

Non-compliance, including tipping off, shall be met with sanctions as provided under the Company's Code of Discipline and this policy.

10. Appendix A, B

502 DY International Building, 1011 Gen. Malvar St cor. San Marcelino St Malate Manila
Website: www.forticareph.com Email Address: customercare.forticare@gmail.com
Trunkline: (02) 5314 CARE (2273) Mobile No. 0927 223 0304

APPLICATION FOR ACCREDITATION PROVIDERS FORM

☐ New Account ☐ Renewal

GENERAL INFORMATION SHEET *Please provide all the information required hereunder.*	**DATE:**
NAME OF ORGANIZATION	
ADDRESS	
DATE OF REGISTRATION/INCORPORATION	**CERTIFICATE/LICENSED TO OPERATE**
TRUNKLINE/TELEPHONE/FAX NO.	**MOBILE NUMBER**
EMAIL ADDRESS	**WEBSITE/FB PAGE**

CONTACT PERSON/S

COMPLETE NAME/S	DESIGNATION	CONTACT DETAILS MOBILE & EMAIL ADDRESS

AUTHORIZED SIGNATORIES

COMPLETE NAME/S	DESIGNATION	CONTACT DETAILS MOBILE & EMAIL ADDRESS

LIST OF AFFILIATED BRANCHES

BRANCH/S	ADDRESS	CONTACT PERSON / CONTACT DETAILS

DECLARATION

I hereby certify that all information stated above are true and correct. I understand that this information will be handle by authorized personnel only and shall be treated with strict confidentiality.

_____
NAME AND SIGNATURE

To be filled out by Forticare Providers Division

Checklist of Requirements:

- ☐ Accomplished Mutual Accreditation Contract-MOA (4 copies)
- ☐ Company Profile
- ☐ SEC Certification
- ☐ BIR Certification
- ☐ Copy of Hospital/Clinic Accreditation and Certification to Operate
- ☐ Latest Audited Financial Statement
- ☐ Updated Business Permit
- ☐ Photocopy of valid IDs for Authorized Signatory
- ☐ Hospital/Clinic Procedure Rates
- ☐ Other _____

Check By: _____
Name/Signature/Date

Noted By: _____
Name/Signature/Date

For more information you may contact the following:

Providers Department
Tel No. (02) 5314 2273 local 115
Mobile No. 09277435328
Email Address: providers.forticare@gmail.com

Admin & Client Services Department
Tel No. (02) 5314 2273 local 120
Mobile No. 09272230304
Email Address: mcj.forticare@gmail.com

INDICATORS OF SUSPICIOUS TRANSACTIONS

1. A request by a customer to enter into an HMO agreement(s) where the source of the funds is unclear or not consistent with the customer's apparent standing;
2. A sudden request for a significant purchase of a lump sum contract with an existing customer whose current contracts are small and of regular payments only;
3. A proposal which has no discernible purpose and a reluctance to divulge a "need" for making the investment;
4. A proposal to purchase and settle by cash;
5. A proposal to purchase by utilizing a cheque drawn from an account other than the personal account of the proposer;
6. The prospective customer who does not wish to know about investment performance but does enquire on the early cancellation/surrender of the particular contract;
7. A customer establishes a ' large policy and within a short time cancels the policy, requests the return of the cash value payable to a Third Party;
8. Early termination of a product, especially in a loss;
9. A customer applies for a policy relating to business outside the customer's normal pattern of business;
10. A customer requests for purchase of policy in an amount considered to be beyond his apparent need;
11. A customer attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments;
12. A customer refuses, or is unwilling, to provide an explanation of the financial activity, or provides explanation assessed to be untrue;
13. A customer is reluctant to provide normal information when applying for an HMO agreement, provides minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify;
14. Delay in the provision of information to enable verification to be completed;
15. Opening accounts with the customer's address outside the local service area;
16. Opening accounts with names like other established business entities;
17. Attempting to open or operating accounts under a false name;
18. Any transaction involving an undisclosed party;
19. A transfer of the benefit of a product to an apparently unrelated third party;
20. A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer or the right to payment could be transferred simply by signing an endorsement on the policy);
21. The customer accepts very unfavorable conditions unrelated to his health or age;
22. An atypical incidence of pre-payment of premiums;
23. Premiums have been paid in one currency and requests for claims to be paid in another currency;
24. Activity is incommensurate with that expected from the customer considering the information already known about the customer and the customer's previous financial activity. (For individual customers, consider customer's age, occupation, residential address, general appearance, type, and level of previous financial activity. For corporate customers, consider type and level of activity);
25. Any unusual employment of an intermediary during some usual transaction or formal activity e.g. payment of claims or high commission to an unusual intermediary;

26. A customer appears to have HMO agreements with several institutions;
27. The customer who is based in non-co-operative countries designated by the FATF from time to time or in countries where the production of drugs or drug trafficking may be prevalent;
28. The customer who is introduced by an overseas agent, affiliate, or other company that is based in non-cooperating countries designated by the FATF from time to time or in countries where corruption or the production of drugs or drug trafficking may be prevalent;
29. Unexpected changes in employee characteristics, e.g. lavish lifestyle or avoiding taking holidays;
30. Unexpected change in employee or agent performance, e.g. the salesperson selling products has a remarkable or unexpected increase in performance;
31. Consistently high activity levels of single premium business far more than any average company expectation;
32. The use of an address which is not the customer's permanent address, e.g. utilization of the salesman's office or home address for the dispatch of customer documentation; and
33. Any other indicator as may be detected by the ICREs from time to time.