ASIA PACIFIC MEDICAL CENTER ILOILO

Data Privacy and Information Security Committee Charter

This Charter was approved and adopted on **16 July 2023** by the Board of Directors of APMC Iloilo to its By-Laws and Revised Manual on Corporate Governance.

SECTION 1. DEFINITIONS

1.1 Defined Terms

The following terms are used in this Charter with the respective meanings ascribed to such terms below, unless the context otherwise requires:

"Advisor"	shall have the meaning ascribed to such term in Section 3.1(b), and which shall include the Chief Information Security Advisor;
"Board"	means the Board of Directors of the Company, the governing body that exercises the corporate powers of the Company, conducts all its business, and controls its properties;
"By-Laws"	means the By-Laws of the Company and all amendments thereto;
"Chairman"	means the Chairman of the Data Privacy and Information Security Committee;
"Chief Information Security Advisor" or "CISA"	means the Chief Information Security Advisor that APMC-Iloilo may engage from time to time, and who shall assist APMC Iloilo in (a) improving, developing and implementing Information Security and cyber security-related policies, processes and technologies; (b) ensuring the compliance of APMC Iloilo with all applicable laws, regulations, and standards; (c) managing cybercrime-related cases filed for and against MPIC; (d) developing and maintaining partnerships with the Government and other private entities for close collaboration in the campaign against cyber threats and/or cybercrimes foreign and domestic; and (e) ensuring alignment of all APMC Iloilo on Information Security and cyber security- related practices;
"Committee"	means the Data Privacy and Information Security Committee of the Board, as constituted from time to time;
"Company" or "APMC Iloilo"	means Asia Pacific Medical Center-Iloilo, Inc.
"Data Privacy"	means the implementation of programs, policies, measures, methods, and procedures to safeguard personal data and to respect the right to privacy of a data subject;

"Data Privacy Officer" or "DPO"	means the Data Privacy Officer of APMC Iloilo, who is responsible for ensuring APMC Iloilo's compliance with the Data Privacy Act of the Philippines and other Privacy Laws;
"Director"	means a member of the Board duly elected in accordance with law and the By-Laws;
"Employees"	means the employees of the Company including its Officers;
"Independent Director"	shall have the meaning ascribed to such term under the Revised Corporation Code and the Securities Regulation Code, as may be amended from time to time;
"Information Security"	means the implementation of proactive measures to safeguard the information assets of APMC Iloilo from unauthorized use, modification, and/or destruction by preserving the confidentiality, integrity, and availability of said information assets;
"Management"	means the members, including the Chairman, of the Committee, as appointed by the Board from time to time;
"Members"	means the members, including the Chairman, of the Committee, as appointed by the Board from time to time;
"Officers"	means the officers of the Company with the rank of Assistant Vice President and above or who are appointed as such by the Board;
"Revised Corporation Code"	means Republic Act No. 11232, known as the "Revised Corporation Code of the Philippines";
"Securities Regulation Code"	means Republic Act No. 8799, known as "The Securities Regulation Code";
"this Charter"	means this Data Privacy and Information Security Committee Charter, including its Schedule and Annexes, as the same may be amended from time to time; and
"year"	means a calendar year.

1.2 Interpretation

(a) Unless the context otherwise requires:

1.3 Interpretation

(a) Unless the context otherwise requires:

(i) words in the singular include the plural, and *vice versa;* and

(ii) words importing any gender include all genders.

(b) The word "writing", or any cognate expression, includes a reference to any communication effected by electronic message, facsimile transmission, or any mode of reproducing words in a legible and non-transitory form.

(c) A reference to a statute or statutory provision shall be construed as a reference to that statute or statutory provision as from time to time amended, modified or reenacted, any repealed statute or statutory provision which it re-enacts, and any order, rule or regulation made under the relevant statute or statutory provision.

(d) The headings in this Charter are inserted solely for convenience of reference and shall not limit or affect the interpretation of the provisions hereof.

SECTION 2. PURPOSES, DUTIES AND POWERS

2.1 The Committee shall have the purposes, duties and powers set out in the Schedule attached hereto and such other duties and powers as may be delegated to the Committee by the Board, subject to such limitations as the Board may determine and notify to the Committee.

2.2 The Committee shall have the resources and authority appropriate to discharge its responsibilities including the authority to engage and obtain advice from experts, counsel, or consultants as it deems appropriate and necessary to carry out its duties, without need for Board approval.

2.3 The Chairman of the Committee and/or any of its Members/ Advisors may meet separately with any member of Management and/or the Data Privacy Officer and/or the Chief Information Security Advisor of APMC Iloilo to discuss any matter that the Committee or any of the foregoing persons believe should be discussed privately. The Committee may also request or require any Employee or Officer of the Company; or the Company's outside counsel; or third-party consultants to attend a meeting of the Committee or to meet with any Member/Advisor/consultant of the Committee.

2.4 As may be requested by the Committee, the Data Privacy Officer and/or the Chief Information Security Advisor shall provide regulatory and technical support for data privacy or information security related matters and functions.

SECTION 3. COMMITTEE STRUCTURE

3.1 Composition

(a) The Committee shall have a minimum of three (3) Members. All Members must be Directors and at least one (1) Member shall be an Independent Director. The Chairman of the Committee shall be chosen from among the Members. The Chairman of the Audit Committee shall not be eligible for election as chairman of this Committee. At least one (1) Member must also be a Member of the Risk Management Committee.

(b) The Board may appoint one or more persons to serve as advisor(s) to the Committee (an "Advisor"). Advisors shall have the right to attend and speak at any meeting of the Committee, but they shall have no right to vote in respect of any action taken by the Committee.

(c) The Chairman of the Committee or any of its Members may be removed from office only by the Board. The Board may delegate to the Committee the appointment, removal and replacements of Advisors.

3.2. Qualifications

(a) Majority of the Members must possess adequate understanding of or experience in the fields of data privacy, information security and/or risk management, preferably in the same industry or of similar business operations as the Company.

(b) The office of a Member shall *ipso facto* be vacated:

(i) if he resigns his office as a Member;

(ii) if he is removed by a resolution of the Board;

(iii) if he becomes of unsound mind;

(iv) if he is convicted of a crime punishable by prision correctional or higher; or

(v) if he is subsequently disqualified under the terms of this Charter and other applicable laws, rules, and regulations from becoming a Member.

If upon determination by the Board or its Nomination Committee, a Member who is a Director ceases to possess any of the qualifications for directorship or becomes disqualified from directorship based on any grounds for disqualification set forth under applicable laws and regulations and the Company's By-Laws and relevant Policies, the Board shall make such appointments in order to meet the required composition of the Committee as set forth in Section 3.1(a).

SECTION 4. COMMITTEE PROCEDURES

4.1 Meetings

(a) The Committee shall hold meetings at such times and places as it considers appropriate provided that at least two (2) meetings shall be held each year.

(b) Meetings of the Committee shall be convened by the Chairman of the Committee as and when he considers appropriate or upon the request of a majority of the Members.

(c) A Committee meeting shall be convened upon notice in writing three (3) days prior to the meeting and specifying the place, date, and time for the meeting and the matters to be discussed at the meeting.

(d) Subject to Section 4.1(i), notwithstanding that a meeting is called by shorter notice, it shall be deemed to have been duly convened if it is so agreed by the Members present in the meeting at which there is a quorum. A Member may consent to short notice and may waive notice of any meeting of the Committee and any such waiver may be retrospective.

(e) Notice of a meeting of the Committee shall be deemed to be duly served upon a Member/Advisor if it is given to him personally, or sent to him by mail, electronic mail or facsimile transmission to his physical address, email address or facsimile number, as appropriate, given by him to the Secretariat of the Committee in accordance with Section 4.1(d) above.

(f) The quorum for a meeting of the Committee shall be at least a majority of the Members present throughout the meeting.

(g) Resolutions at a meeting of the Committee at which there is a quorum shall be passed by a simple majority of votes of the Members present at such meeting.

(h) Each Member, including the Chairman of the Committee, shall have one (1) vote.

(i) In case of an equality of votes, the Chairman of the Committee shall not have a second or casting vote.

(ii) A resolution in writing signed by all Members shall be as valid and effective for all purposes as a resolution of the Committee passed at a meeting of the Committee duly convened, held and constituted. A written notification of confirmation of such resolution in writing sent by a Member shall be deemed to be his signature to such resolution in writing for such purpose. Such resolution in writing may consist of several documents, each signed by one or more Members.

(i) If, within thirty (30) minutes from the time appointed for a meeting of the Committee, a quorum is not present, the meeting shall stand adjourned to the same day in the next week at the same time and place, or to such other day, time and place as the Chairman of the meeting may determine.

(j) Members and Advisors of the Committee may participate in a meeting of the Committee through teleconference or video conference by means of which all persons participating in the meeting can hear each other.

4.2 Minutes and Records

(a) The Corporate Secretary or any person designated by him shall act as the Secretariat of the Committee. The Secretariat shall prepare the agenda of each Committee meeting in coordination with the Chairman, collate documents pertaining to the matters in the agenda, prepare minutes of the meetings of the Committee, and/or recall sheets of decisions made during meetings of the Committee, and keep records of the Committee.

(b) The Committee shall cause records to be kept for the following:

(i) appointments and resignations of the Members/Advisors;

(ii) all agenda and other documents sent to the Members/Advisors; and

(iii) minutes of proceedings and meetings.

(c) Any such records shall be open for inspection by any Member/Advisor upon reasonable prior notice during usual office hours of the Company.

(d) Minutes of any meeting of the Committee, if purported to be signed by the Chairman of such meeting, or by the Chairman of the next succeeding meeting, shall be conclusive evidence of the proceedings and resolutions of such meeting.

SECTION 5. REMUNERATION OF MEMBERS/ADVISORS

No fees or other remuneration shall be payable to the Members/ Advisors of the Committee in respect of their services provided in connection with the Committee or in respect of their attendance at meetings of the Committee, save and except fees or remuneration authorized and approved by the Board for such purposes. In the case of a Member who is an Independent Director, no fees or compensation shall be paid directly or indirectly to such Member or his firm for consultancy or advisory services rendered directly by the Member or indirectly through his firm even if such Member is not the actual service provider. However, this prohibition shall not apply to ordinary compensation paid to such Member or his firm in respect of any other supplier or other business relationship or transaction that the Board has already determined to be at arm's length terms and immaterial for purposes of its basic Member's independence analysis.

SECTION 6. AMENDMENT

This Charter shall not be amended, altered, or varied unless such amendment, alteration or variation shall have been approved by a resolution of the Board.

SCHEDULE OF PURPOSES, FUNCTIONS, AND DUTIES OF THE DATA PRIVACY AND INFORMATION SECURITY COMMITTEE

Purposes

The primary purpose of the Committee is to assist the Board in fulfilling its functions to perform oversight of and give strategic direction to the governance functions relating to data privacy and information security related matters. These functions include:

1. Promoting effective data privacy and information security governance within the Company and its subsidiaries and investee companies;

2. Reviewing and approving the Company's strategic plans on data privacy and information security to protect Company's assets commensurate with the risk appetite of the organization and to ensure that the strategic plans are aligned with overall business objectives of the Company;

3. Holding Management accountable for compliance with regulatory standards and best practices on data privacy and information security;

4. Fostering a company culture where privacy and information security is considered "the new normal" by all Employees, leading by example, and demonstrating the right aptitude and behavior; and

5. Overseeing Management's adoption and implementation of a system for identifying, assessing, monitoring and managing enterprise-wide data privacy and information security risk.

Functions and Duties

To carry out its purposes, the Committee shall have the following duties and powers:

1. Overseeing the compliance and adherence by the Company with all applicable laws and regulations on data privacy and information security pursuant to which the Company conducts its operations and business activities. In matters relating to interpretation of any law, issuance, or policy relating to Data Privacy and/or Information Security, the Committee shall ensure that the inputs of the Data Privacy Officer and/or the Chief Information Security Advisor, as appropriate, are solicited and considered;

2. In coordination with Management:

    (a) Reviewing and discussing Management's reports, which shall contain the Company's management of enterprise-wide data privacy and information security risks, including frameworks, structures, policies, standards, and processes in identifying, assessing, monitoring, managing, reporting and communicating and enforcing data privacy and information security risk management policies;

(b) Reviewing and discussing Management's reports on the Company's data privacy and information security risk profile, with focus on known or emerging major risk exposures;

(c) Reviewing and discussing the steps proposed to be taken by Management to monitor and manage data privacy and information security risks, including adequacy of resources; training of the workforce; administrative, physical, and technical safeguards; and an incident management framework;

(d) Establishing and maintaining effective lines of accountability, responsibility, and authority for protecting information assets by reviewing and approving privacy and information security organizational changes, processes, and policies;

(e) Overseeing the effectiveness and status of the Company's privacy and security programs and help balance conflicting priorities and resource demands;

(f) Reviewing and approving at least annually the risk appetite and risk tolerance of the Company and the risk management objectives and strategies with respect to data privacy and information security to be recommended to the Board for approval;

(g) Overseeing the coordination across the MPIC Group to ensure a coherent data privacy and information security strategy; and

(h) Monitoring data privacy and/or cybersecurity risks and issues that may arise in the Company's subsidiaries and investee companies, and recommending actions to be taken to address the same.

3. Periodically obtaining reasonable assurance from Management that:

(a) The Company's data privacy and information security risk management framework, processes and policies are comprehensive, updated and effective;

(b) There are adequate plans in place to address data breaches and security incidents, including insurance and public relations plans;

(c) The Company, as a publicly-listed company, complies with its unique disclosure requirements without overlooking its fiduciary privacy protection obligations; and

(d) The Company's data privacy and information security posture is effective and sustainable in terms of, among others, enhancing opportunities, creating business value, and managing threats, including issues that may arise from changing trends in regulatory landscape, developments in the industry and innovations in technology.

4. Periodically receiving reports from Management on the status of any regulatory actions against the Company, as well as pending cases filed by and against the Company arising from data privacy and/or information security issues;

5. Reporting to the Board, independent of Management, the Committee's views as to whether there are any significant gaps in Management's data protection and information security capabilities and the status of any initiatives to address those gaps;

6. In consultation with the President/Chief Executive Officer and the Chairman of the Data Privacy and Information Security Committee, reviewing the appointment/replacement and performance of the Data Privacy Officer and/or Chief Information Security Advisor;

7. Reporting the Committee's activities to the Board at least once each year and making such recommendations with respect thereto and other matters as the Committee may deem necessary or appropriate;

8. Conducting an annual evaluation of the Committee's performance, which evaluation must compare the performance of the Committee with the requirements of this Charter and the goals and objectives of the Committee for the relevant year, and reporting to the Board the results of such evaluation; provided that such report to the Board may take the form of an oral report by the Chairman of the Committee or any other Member designated by the Committee to make such report; and

9. Reviewing this Charter annually and recommending changes or improvements hereto that the Committee may deem necessary or desirable, including those that are necessary to respond to new risk-oversight needs and changes in regulatory and other requirements.