DATA PRIVACY POLICY

I. PURPOSE

1.1. To govern the implementation of the Data Privacy Rules and Regulations as mandated by Republic Act No. 10173 or the "Data Privacy Act of 2012" at Maayo Well.

1.1.1. Maayo Well pledges to protect personal information.

1.1.2. Maayo Well shall take steps to protect personal information from theft, loss or unauthorized access, copying, modification, use, disclosure or disposal.

1.1.3. Maayo Well shall take steps to ensure that anyone who performs services on Maayo Medical Clinic's behalf respects privacy rights and only uses or discloses personal information for permitted purposes.

1.1.4. Maayo Well shall promptly investigate all complaints regarding our compliance with the DPA. All privacy complaints shall be treated in a confidential manner.

II. SCOPE

2.1. This policy will cover all processes related to the handling of Data. This includes data collection, data storage, and disposal of data. This also encompasses certain administrative sanctions relevant to the non-compliance of the policy.

III. DEFINITION OF TERMS

3.1. Data Privacy Act refers to Republic Act No. 10173 or the Data Privacy Act of 2012 and its implementing rules and regulations;

3.2. Data Subject refers to an individual whose personal, sensitive personal, or privileged information is processed;

3.3. Office refers to the Maayo Medical Clinic QM Office (Maayo Medical Clinic);

3.4. Personal Data collectively refers to personal information, sensitive personal

information, and privileged information;

3.5. Personal Information refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;

3.6. Processing refers to any operation or set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;

3.7. Privileged information refers to any and all forms of personal data, which, under the Rules of Court and other pertinent laws constitute privileged communication;

3.8. Security incident is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place;

3.9. Sensitive Personal Information refers to personal data:

3.9.1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

3.9.2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;

3.9.3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

3.9.4. Specifically established by an executive order or an act of Congress to be kept classified.

IV. POLICY

4.1 Organizational Security Measures

4.1.1 Data Privacy Officer

4.1.1.1 A Data Privacy Officer (DPO, for brevity) shall be appointed by the Office. The DPO shall be chosen from one of the officers of the clinic and will work closely with the Quality and Risk Management Office (Privacy Information Controller) and Information Technology (Privacy Information Processor) Department.

4.1.2. The DPO is responsible for ensuring the Office's compliance with applicable laws and regulations protection of data privacy and security. The DPO's functions and responsibilities shall particularly include, among others:

4.1.2.1. Monitoring the Office's personal data processing activities in order to ensure compliance with applicable personal data privacy laws and regulations, including the conduct of periodic internal audits and review to ensure that all the Office's data privacy policies are adequately implemented by its employees and authorized agents;

4.1.2.2. Acting as a liaison between the Office and the regulatory and accrediting bodies, and is in charge of the applicable registration, notification, and reportorial requirements mandated by the Data Privacy Act, as well any other applicable data privacy laws and regulations;

4.1.2.3. Developing, establishing, and reviewing policies and procedures for the exercise by data subjects of their rights under the Data Privacy Act and other applicable laws and regulations on personal data privacy;

4.1.2.4. Acting as the primary point of contact whom data subject may coordinate and consult with for all concerns relating to their personal data;

4.1.2.5 Formulating capacity building, orientation, and training programs for employees, agents or representatives of the Office regarding personal data privacy and security policies;

4.1.2.6 Preparing and filing the annual report of the summary of documented security incidents and personal data breaches, if any, as required under the Data Privacy Act, and of compliance with other requirements that may be provided in other issuances of the National Privacy Commission.

4.2. Data Privacy Principles

4.2.1. All processing of personal data within the Office should be conducted in compliance with the following data privacy principles as espoused in the Data Privacy Act:

4.2.2.1. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data by the Office, including the risks and safeguards involved, the identity of persons and entities involved in processing his or her personal data, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

4.2.2.2. Legitimate purpose. The processing of personal data by the Office shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

4.2.2.3. Proportionality. The processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed by the Office only if the purpose of the processing could not reasonably be fulfilled by other means.

4.3. Rights of the Data Subject

4.3.1. As provided under the DPA, data subjects have the following rights in connection with the processing of their personal data: right to be informed, right to object, right to access, right to rectification, right to erasure or blocking, and right to damages. Employees and staff of the Office are required to strictly respect and obey the rights of the data subjects. The DPO shall be responsible for monitoring such compliance and developing the appropriate disciplinary measures and mechanism.

4.3.2. Right to be informed

4.3.2.1. The data subject has the right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed.

4.3.2.2. The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the records of the Office, or at the next practical opportunity:
1. Description of the personal data to be entered into the system;
2. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
3. Basis of processing, when processing is not based on the consent of the data subject;
4. Scope and method of the personal data processing;
5. The recipients or classes of recipients to whom the personal data are or may be disclosed or shared;
6. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
7. The identity and contact details of the DPO;
8. The period for which the information will be stored; and
9. The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the National Privacy Commission.

4.3.3. Right to Object

4.3.3.1. The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

4.3.3.2 When a data subject objects or withholds consent, the Office shall no longer process the personal data, unless:
1. The personal data is needed pursuant to a subpoena;
2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the Office and the data subject; or
3. The personal data is being collected and processed as a result of a legal obligation.

4.3.4. Right to Access

4.3.4.1 The data subject has the right to reasonable access to, upon demand, the following:

1. Consent of his or her personal data that were processed;
2. Sources from which personal data were obtained;
3. Names and addresses of recipients of the personal data;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal data to recipients, if any;
6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
7. Date when his or her personal data concerning the data subject were last accessed and modified; and
8. The designation, name or identity, and address of the DPO.

4.3.5 Right to Rectification

4.3.5.1. The data subject has the right to dispute the inaccuracy or error in the personal data, and the Office shall correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the Office shall ensure the accessibility of both the new and the retracted personal data and the simultaneous receipt of the new and the retracted personal data by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

4.3.6. Right to Erasure of Blocking

4.3.6.1. The data subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his or her personal data from the Office's filing system.

4.3.6.2. This right may be exercised upon discovery and substantial proof of any of the following:

1. The personal data is incomplete, outdated, false, or unlawfully obtained;
2. The personal data is being used for purpose not authorized by the data subject;
3. The personal data is no longer necessary for the purposes for which they were collected;

4. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing by the Office;
5. The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
6. The processing is unlawful; or
7. The data subject's rights have been violated

4.3.7. Transmissibility of Rights of Data Subjects

4.3.7.1. The lawful heirs and assigns of the data subject may invoke the rights of the data subject to which he or she is an heir or an assignee, at any time after the death of the data subject, or when the data subject is incapacitated or incapable of exercising his/her rights.

4.3.8. Data Portability

4.3.8.1. Where his or her personal data is processed by the Office through electronic means and in a structured and commonly used format, the data subject shall have the right to obtain a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The DPO shall regularly monitor and implement the National Privacy Commission's issuances specifying the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

4.4. Data Breaches and Security Incidents

4.4.1. Data Breach Notification

4.4.1.1. All employees and agents of the Office involved in the processing of personal data are tasked with regularly monitoring for signs of a possible data breach or security incident. In the event that such signs are discovered, the employee or agent shall immediately report the facts and circumstances to the DPO within twenty-four (24) hours from his or her discovery for verification as to whether or not a breach requiring notification under the Data Privacy Act has occurred as well as for the determination of the relevant circumstances surrounding

the reported breach and/or security incident. The DPO shall notify the National Privacy Commission and the affected data subjects pursuant to requirements and procedures prescribed by the DPA.

4.4.1.2. The notification to the DPA and the affected data subjects shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken by the Office to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach and the name and contact details of the DPO. The form and procedure for notification shall conform to the regulations and circulars issued by the National Privacy Commission, as may be updated from time to time.

4.4.2. Breach Reports

4.4.2.1. All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the personal information controller. In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the National Privacy Commission. A general summary of the reports shall be submitted by the DPO to the National Privacy Commission annually.

4.5. Outsourcing and Subcontracting Agreements

4.5.1. Any personal data processing conducted by an external agent or entity (third-party service provider) on behalf of the Office should be evidenced by a valid written contract with the Office. Such contract should expressly set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the Office, and the geographic location of the processing under the contract.

4.5.2. The fact that the Office entered into such contract or arrangement does not give the said external agent or entity the authority to subcontract to another entity the whole or part of the subject matter of said contract or arrangement, unless expressly stipulated in writing in the same contract or evidenced by a separate written consent/agreement of the Office. The subcontracting

agreement must also comply with the standards/criteria prescribed by the immediately preceding paragraph.

4.5.3. In addition, the contract and the subcontracting contract shall include express stipulations requiring the external agent or entity (including the subcontractor) to:

4.5.3.1. Process the personal data only upon the documented instructions of the Office, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;

4.5.3.2. Ensure that an obligation of confidentiality is imposed on persons and employees authorized by the external agent/entity and subcontractor to process the personal data;

4.5.3.3. Implement appropriate security measures;

4.5.3.4. Comply with the Data Privacy Act and other issuances of the National Privacy Commission, and other applicable laws, in addition to the obligations provided in the contract or other legal act with the external party;

4.5.3.5. Not engage another processor without prior instruction from the Office: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;

4.5.3.6. Assist the Office, by appropriate technical and organizational measures, and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;

4.5.3.7. Assist the Office in ensuring compliance with the Data Privacy Act and other issuances of the National Privacy Commission, taking into account the nature of processing and the information available to the external party who acts as a personal information processor as defined under the Data Privacy Act;

4.5.3.8. At the choice of the Office, delete or return all personal data to it after the end of the provision of services relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the Data Privacy Act or another applicable laws or regulations;

4.5.3.9. Make available to the Office all information necessary to demonstrate compliance with the obligations laid down in the Data Privacy Act, and allow for and contribute to audits, including inspections, conducted by the Office or another auditor mandated by the latter; and

4.5.3.10. Immediately inform the Office if, in its opinion, an instruction violates the Data Privacy Act or any other issuance of the National Privacy Commission.

4.6. Non-adherence to Policies and Procedures

4.6.1. An Improvement Action Form (IAF) shall be issued to any staff/division not adhering to the foregoing Data Privacy Manual.

4.6.2. Staff with a single non-conformity but with detrimental repercussion to the clinic's operation and/or with recurrent non-conformities to the Data Privacy Manual shall be subjected to disciplinary actions following existing clinic rules and regulations.

4.6.3. After due process, staff who commits Data Privacy Act non-conformity with detrimental repercussion to the clinic's operation and reputation shall be subjected to the Penalties in reference to the Data Privacy Act of 2012;

4.6.3.1. Unauthorized Processing of Personal Information and Sensitive Personal Information. – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.(b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law. Data Privacy Act of 2012 Republic Act No. 10173 Section 25.

4.6.3.2. Accessing Personal Information and Sensitive Personal Information Due to Negligence. – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one

(1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.(b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law. Data Privacy Act of 2012 Republic Act No. 10173 Section 26.

4.6.3.3. Improper Disposal of Personal Information and Sensitive Personal Information. – (a) The improper disposal of personal information shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection. b) The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection. Data Privacy Act of 2012 Republic Act No. 10173 Section 27.

4.6.3.4. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. – The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven

(7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws. Data Privacy Act of 2012 Republic Act No. 10173 Section 28.

4.6.3.5. Unauthorized Access or Intentional Breach. – The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored. Data Privacy Act of 2012 Republic Act No. 10173 Section 29.

4.6.3.6. Concealment of Security Breaches Involving Sensitive Personal Information. – The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach. Data Privacy Act of 2012 Republic Act No. 10173 Section 30.

4.6.3.7. Malicious Disclosure. – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00). Data Privacy Act of 2012 Republic Act No. 10173 Section 31.

4.6.3.8. Unauthorized Disclosure. – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than

Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00). Data Privacy Act of 2012 Republic Act No. 10173 Section 32.

4.6.3.9. Combination or Series of Acts. – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00). Data Privacy Act of 2012 Republic Act No. 10173 Section 33.

4.6.3.9.1. Extent of Liability. – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.
Data Privacy Act of 2012 Republic Act No. 10173 Section 34.

4.6.3.9.2. Large-Scale. – The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal information of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions. Data Privacy Act of 2012 Republic Act No. 10173 Section 35.

4.6.3.9.3. Restitution. – Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code. Data Privacy Act of 2012 Republic Act No. 10173 Section 33

V. PROCEDURE

5.1. Data Processing Records

5.1.1 Adequate records of the Office's personal data processing activities shall be maintained at all times. The DPO, with the cooperation and assistance of the Information Technology (Office's Electronic Medical Record (EMR, for brevity) shall be responsible for ensuring that these records are kept up-to-date. These records shall include, at the minimum:

5.1.1.1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing;

5.1.1.2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;

5.1.1.3. General information about the data flow within the Office, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data;

5.1.1.4. A general description of the organizational, physical, and technical security measures in place within the Office; and

5.1.1.5. The name and contact details of the DPO as well as any other staff members accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

5.2. Management of Human Resources

5.2.1. The DPO, with the cooperation of the Office's Human Resources Department (HRD, for brevity), shall develop and implement measures to ensure that all the Office's staff who have access to personal data will strictly process such data in compliance with the requirements of the Data Privacy Act and other applicable laws and regulations. These measures may include drafting new or updated relevant policies of the Office and conducting training programs to educate employees and agents on data privacy related concerns.

5.3. Employment Agreements

5.3.1. The DPO shall ensure that all employment agreements reflect appropriate clauses indicating the employee's informed consent to:

5.3.1.1 The processing of his or her personal data, for purposes of maintaining the Office's records;

5.3.1.2. A continuing obligation of confidentiality on the employee's part in connection with the personal data that he or she may encounter during the period of employment with the Office. This obligation shall apply even after the employee has left the Office for whatever reasons.

5.4. Management of Medical Records and Confidentiality of Patient Data

5.4.1 The DPO with the cooperation of the Office's Medical Records Department shall develop and implement measures to ensure that all Health Care Workers who have access to the patients' personal data will strictly process data in compliance with the requirements of the Data Privacy Act and other applicable laws and regulations. Furthermore, any data gathered from the patient should be treated with utmost confidentiality and should only be asked if and when necessary.

5.4.2 Staff respects patient privacy by not posting confidential information in treatment/diagnostic/consultation areas and reception areas and by not discussing patient-related information in public places.

5.4.3. Patient Chart contains medical and other health information which is important for understanding the patient condition and his or her need for medical attention. The clinic respects such information as confidential and has implemented policies and procedures that protect such information from loss or misuse.

5.4.4. Consent to release information should be complied prior to the release of any documents related to the management of treatment of patient and other services deemed necessary for such consent.

5.5. Consent to Care

5.5.1. The DPO shall ensure that all services performed which entails data gathering is agreed by the patient or the responsible party (SO) prior to actual giving of the service thru signing of the Patient Consent.

5.5.2. A general consent for treatment is obtained from patient during registration.

5.5.3. Additional consent will be required for certain procedures or treatments with high risks.

5.6. Data Collection Procedures

5.6.1. The DPO, with the assistance of the Office's Administrative Directorate, Medical Directorate, Allied Medical Services, Nursing Services, Human Resource Division, and Finance Directorate and any other departments of the Office responsible for the collection and processing of personal data, shall document the Office's personal data collection and processing procedures. The DPO shall ensure that such procedures are updated and that the consent of the data subjects (when required by the DPA or other applicable laws or regulations) is properly obtained. Such procedures shall also be regularly monitored, modified, and updated to ensure that the rights of the data subjects are respected, and that processing thereof is done fully in accordance with the DPA and other applicable laws and regulations.

5.7. Data Retention Schedule

5.7.1. Subject to applicable requirements of the DPA and other relevant laws and regulations, personal data shall not be retained by the Office for a period longer than necessary and/or proportionate to the purposes for which such data was collected. The DPO shall be responsible for developing measures to determine the applicable data retention schedules, as well as to safeguard the destruction and disposal of such personal data in accordance with the DPA and other applicable laws and regulations.

5.7.2. The retention period for each specific document is part of the Management of Information standard

5.8. Physical Security Measures

5.8.1. The DPO shall develop and implement policies and procedures for the Office to monitor and limit access to, and activities in, the offices of the

Administrative Directorate, Medical Directorate, Allied Medical Services, Nursing Services, Human Resource Division, and Finance Directorate, as well as any other departments and/or workstations in the Office where personal data is processed, including guidelines that specify the proper use of, and access to, electronic media.

5.8.2. The design and layout of the office spaces and work stations of the abovementioned departments, including the physical arrangement of furniture and equipment, shall be periodically evaluated and readjusted in order to provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public.

5.8.3. The duties, responsibilities, and schedules of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time. Further, the rooms and workstations used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

5.9. Technical Security Measures

5.9.1. The DPO, with the cooperation and assistance of Administrative Directorate, shall continuously develop and evaluate the Office's security policy with respect to the processing of personal data. The security policy should include the following minimum requirements:
5.9.1.1. Safeguards to protect the Office's computer network and systems against accidental, unlawful, or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access;
5.9.1.2. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of the Office's data processing systems and services;
5.9.1.3. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in the Office's computer network and system, and for taking preventive, corrective, and mitigating actions against security incidents that can lead to a personal data breach;
5.9.1.4. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
5.9.1.5. A process for regularly testing, assessing, and evaluating the effectiveness of security measures; and

5.9.1.6 Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

VI. APPENDICES

6.1. For more information about the Maayo Medical Clinic privacy protection practices, or to raise a concern about our privacy protection practices, please contact us:

By mail:
Dr. Manuel Emerson Donaldo
Data Privacy Officer
Maayo Medical Clinic Admin Office
United Nations Avenue cor. Plaridel St.
Alang-Alang, Cebu, Philippines

By telephone:
(+6332)8882662 Loc 1371
By email:
info@maayomedical.com

VII. REFERENCES

7.1. Maayo Well Quality Manual

7.2. Health Privacy Code implementing Administrative Order No. 2016-0002 “Privacy Guidelines for the Implementation of the Philippine Health Information Exchange”

7.3. Joint Commission International Accreditation Standards for Ambulatory care 3rd Edition

7.4. Data Privacy Act of 2012 (Republic Act No. 10173)

7.5. National Privacy Act Tool Kit: a Guide for Management and Data Protection Officers