DEPARTMENT OF HEALTH
DEPARTMENT OF SCIENCE AND TECHNOLOGY
PHILIPPINE HEALTH INSURANCE CORPORATION

HEALTH PRIVACY CODE IMPLEMENTING THE JOINT ADMINISTRATIVE ORDER NO. 2016-0002 "PRIVACY GUIDELINES FOR THE IMPLEMENTATION OF THE PHILIPPINE HEALTH INFORMATION EXCHANGE".

WHEREAS, Joint Administrative Order No. 2016-0002 entitled "PRIVACY GUIDELINES FOR THE IMPLEMENTATION OF THE PHILIPPINE HEALTH INFORMATION EXCHANGE" was approved on January 20, 2016 and took effect on _____, _____ days after its complete publication in a major newspaper of national circulation in the Philippines, implementing Republic Act No. 10173 also known as the Data Privacy Act of 2012.

NOW THEREFORE, the following rules are hereby promulgated:

Part 1: Preliminary

1. Introduction.

Pursuant to the state policy enshrined in the Constitution to provide quality health care to the Filipino people while protecting and promoting the right to privacy, the Department of Health (DOH), in cooperation with the Department of Science and Technology (DOST), Philippine Health Insurance Corporation (PhilHealth), University of the Philippines-Manila (UPM) and the Commission on Higher Education (CHED), established the National eHealth Program (NeHP) that envisions widespread information-technology (IT)-enabled health services by 2020.

Guided by the Philippine eHealth Strategic Framework and Plan, one of the identified eHealth Project is the implementation of the Philippine Health Information Exchange (PHIE). The PHIE is the first major collaborative and convergence endeavor of the Health Cluster, and represents the initial step towards the realization of the National eHealth vision.

The PHIE will enable electronic transmission of healthcare-related data among health facilities, health care providers, health information organizations and government agencies, in accordance with national standards. It will allow different applications to exchange data with each other without loss of semantics and will enable health facilities particularly rural health units, health centers, hospitals, DOH and PhilHealth to communicate with each other effectively and to collaborate with the health care providers in the care of the patients. The development and implementation of the PHIE will enable a patient's medical or health information to follow the patient wherever health care services are provided. Health care providers will be able to exchange patient's medical or health information securely to improve health care delivery and decision making.

2. Title.

This shall be known and cited as the Health Privacy Code of Joint Administrative Order No. 2016-0002, otherwise known as "Privacy Guidelines for the Implementation of the Philippine Health Information Exchange" (Code).

3. Purpose.

This Code is hereby promulgated to prescribe the procedures and guidelines that ensure the protection of the privacy of a patient.

4. Scope of Application.

This code shall apply to the PHIE system, Health Facilities, Health Care Providers, and any natural or juridical person involved in the processing of health information within the PHIE framework.

5. Definition of Terms.

Access	Instruction to, communication with, storing data in, or retrieving data from, a computer system or communication network, or any process or operation that makes use of any resources of such system or network.

Addressable	Flexible specifications allowing the health facility or health care provider to perform one of the following actions: a) Implement the addressable implementation specification; b) Implement one or more alternative security measures to accomplish the same purpose; or c) Not implement either an addressable implementation specification or an alternative.
Alteration	Modification or change, in form or substance, of an existing computer data or program.
Authentication	Process of verifying that an individual, entity or software program accessing the PHIE is the authorized user the individual, entity or program claims to be.
Authorization	Process that determines whether a user has the right to access the PHIE and establishes the privileges associated with such access.
Breach	The unauthorized or impermissible acquisition, access, use, or disclosure of information and can be in the context of the patient and/or institutions.
Cache	A special high-speed storage mechanism which cans either be a reserved section of the main memory or an independent high-speed storage device.
Caching	The process of storing data in a cache.
Computing and Related equipment	Computer network, as well as, telecommunications and peripheral equipment that support the data processing activities of organizations.
Confidentiality	A duty to protect personal data against unauthorized disclosure.
Consent	Any freely-given, specific, informed indication of will, whereby an individual agrees to the collection and processing of personal information relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the individual by a lawful guardian or an agent specifically authorized by the individual to do so.
Data Subject	An individual whose personal, sensitive personal, or privileged information is processed.
Data Processing System	The structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;
Data Protection Officer	An individual who is accountable for ensuring compliance with applicable laws and regulations relating to data privacy and security.
Data Privacy Act or DPA	Republic Act No. 10173, also known as the Data Privacy Act of

	2012.
Data Processor	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Sharing	The disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor.
Decryption	Process of transforming data rendered unreadable by encryption back to its unencrypted form.
De-identification	Removal of identifiers to protect against inappropriate disclosure of personal data.
Digital Signature	A specific type of electronic signature based on public-key cryptography, which is used within a framework known as public-key infrastructure.
Discharge	The release of a patient from a healthcare provider's care, and usually refers to the date when a patient checks out of a health facility or hospital.
Electronic Medical Record	A medical or health record which is received, recorded, transmitted, stored, processed, retrieved or produced electronically through a computer or any other electronic device.
Electronic Signature	Any representation in electronic form that can be used to express intent, including a printed name at the bottom of an e-mail, a digitized copy of a handwritten signature, a biometric mark, a sound, or digital structure.
Emergency	Unforeseen combination of circumstances that calls for immediate life-preserving or quality-of-life preserving actions (e.g., to preserve sight in one or both eyes, hearing in one or both ears, extremities at or above the ankle or wrist).
Encryption	The use of an algorithmic process to transform data into another form such that there is a low probability of assigning meaning thereto without use of a confidential process or key.
Health Care Clearinghouse	A public or private entity that performs any of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data into standard data elements or a standard

	transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. It may include a billing service, repricing company, community health management information system or community health information system, or any other "value-added" networks and switches.
Health Care Provider	A health care institution devoted primarily to the management, treatment and care of patients, or a health care professional, who is any doctor of medicine, nurse, midwife, dentist, or other health care practitioner.
Health Data Warehouse	A repository of the country's de-identified health information within the framework of the Philippine Health Information Exchange.
Health Facility	
Health Information	Personal information and sensitive personal information that relates to an individual's past, present or future physical or mental health condition, including demographic data, diagnosis and management, medication history, health financing record, cost of services and any other information related to an individual's total well-being. <u>For purpose of A.O. 2016-0002, health information refers to personal health information which is individually identifiable information or de-identified health information.</u>
Information and Communication Technology (ICT) systems	Hardware, software, firmware of computers, telecommunications and network equipment or other electronic information handling systems and associated equipment.
Individually Identifiable	Refers to information that contains data that an directly identify the individual or could reasonably be used to identify an individual.
Information System	Application, service, information technology asset, or any other information handling component.
Infrastructure	Facilities and equipment that enable the ICT service, including but not limited to power supply, telecommunications connections and environmental controls.
Inpatient	A patient admitted to a health facility or hospital to receive healthcare services, including room, board and continuous nursing services in a unit area of the facility.
Issuances	Official write-up or documentation of statements, notices, announcements, and communications.

Interception	Listening to, recording, monitoring or surveillance of the content of communications, including procuring the content data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.
Interpersonal Violence	Violence that occurs between family members, intimate partners, friends, acquaintances and strangers, and includes child maltreatment, youth violence, sexual violence and elder abuse.
Medical Privacy or Health Privacy	Right to the protection of a person's health information, which includes personal data, information about a patient's condition as contained in medical records, and communications between healthcare provider and a patient.
Medical Record or Health Record	Primary repository of information concerning patient healthcare, which consists of a compilation of pertinent facts regarding a patient's life history including past and present illnesses and treatments entered by a health professional contributing to the patient's care.
National Privacy Commission or NPC	An independent government agency created under the DPA to administer and implement the provisions of the law, and to monitor and ensure compliance of the Philippines with international standards set for data protection.
Outpatient	A patient who receives medical care or healthcare services without being admitted and does not occupy a bed for any length of time. It may also refer to a patient who consults and receives healthcare services in the healthcare facility without being admitted.
Participating Health Care Provider (PHCP)	Health care providers whose application to participate in the PHIE is approved in accordance with Joint DOH-DOST-PhilHealth A.O. 2016-0001 (Implementation of the PHIE), and any other procedure that may be promulgated by the DOH for participation.
Patient or Client	A person availing of medical consultation, diagnostic examinations, treatment or health care services from a health care provider.
Patient Registry	Organization and processes supporting a patient register
Patient Register	A set of patient records systematized around a particular disease, condition or exposure, and serving "one or more predetermined scientific, clinical or policy purposes".
Personal Information	Any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonable and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual

Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Personal Information Controller	A person or organization that controls the collection, holding, processing or use of personal information, including a person or organization that instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. This term excludes: (a) A person or organization who performs such functions as instructed by another person or organization; and (b) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.
Personal Information Processor	Any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.
Privacy	The right of a person to be free from intrusion or disturbance in one's personal and intimate life or affairs. It includes data privacy, which refers to the right of an individual not to have his or her personal data disclosed using the ability to control what personal data is disclosed, with whom, and for what purpose.
Privilege Communication	Conversation or working relationship which takes place between two parties within the context of a protective relationship such as between healthcare provider and a patient.
Processing	Any operation performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
Publication	The act or process of producing a book, magazine, etc., and thereafter making it available to the public.
Public Health	All organized measures to prevent disease, promote health, and prolong life across the population. Its activities aim to provide conditions in which people can be healthy. They focus on entire populations, not on individual patients or diseases.
Public Health Emergency	An occurrence or imminent threat of an illness or health condition, cause by bio terrorism, epidemic or pandemic disease, or a novel and highly fatal infectious agent or biological toxin, that poses a substantial risk of a significant number of human facilities or

	incidents or permanent long-term disability.
Required	Specifications that must be implemented.
Security	The organization, technical and physical measures to ensure the safety and protection of the health information.
Security Incident	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.
Sensitive Personal Information	Personal information: (a) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (b) 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 person, the disposal of such proceedings, or the sentence of any court in such proceedings; (c) Issued by government agencies peculiar to an individual which includes but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; (d) Specifically established by an executive order or an act of Congress to be kept classified.
Sharing	The process that allows the PHCP to access a patient's health information from the framework.
Shared Health Record	An operational, real-time, transactional data source that serves as a means for allowing different services to share health information stored in a centralized data repository. It contains a subset of normalized data for a patient from various systems such as but not limited to, Electronic Medical Record (EMR).
Social Media	Electronic communication, websites or applications through which users connect, interact, or share information or other content with other individuals who collectively form part of an online community. This includes Facebook, Twitter, Google+, Instagram, LinkedIn, Pinterest, Blogs, and other Social Networking Sites.
Third Party	Any person, entity or institution other than the patient, healthcare provider or health facility, or any other duly authorized personal information processor or person desiring to have access to patient's health information (i.e. HMOs, researchers, among others).

Part 2: Health Information Privacy Rules

Rule 1
Collection and Processing of Health Information

1. *Consent.*
The consent shall conform to the requirements or characteristics of a valid informed consent which consist of the following:

- **A. *Competence-*** of sound mind, at least 18 years old, and not under the influence of drugs or liquor;
- **B. *Amount and Accuracy of Information-*** Relevant factual data about a procedure and/or treatments, its benefits, risks, and possible complications or outcomes;
- **C. *Patient Understanding-*** Education, language or dialect;
- **D. *Voluntariness-*** Make an autonomous decision without force or intimidation, and understands that he/she can withdraw consent anytime without consequence;

1.1. *For Persons with Disabilities (PWDs).*
Use of appropriate means of communication such as verbal or sign language.

1.2. *Persons to Obtain Consent.*
Consent shall be obtained by a duly authorized staff who shall be responsible for informing the patients regarding the implementation of the PHIE, and the validation of patient information.

1.3. *Persons to Give Consent.*
Consent shall be given by a patient of legal age and sound mind, or otherwise incapacitated to give consent, any of the following in the order stated hereunder, can give consent:

(a) Immediate relatives within the 3rd degree of consanguinity based on hierarchy: provided, that in the case of minors, either parent may give consent, unless the married, in which case, preference shall be given to the mother;
(b) Cohabitant partner for a minimum of one (1) year or actual and identified guardian of the patient;
(c) Social worker;
(d) Attending physician.

Provided, that if a patient has a duly executed advance directive or power of attorney for healthcare, the same shall be given effect.

1.4. *When to Get Consent.*
Upon order of discharge/prior to discharge from the health facility.

1.5. *The Consent Form.*

The standard "Consent for Participation to PHIE" shall be used by participating health care providers.

1.6. *Valid formats of consent.*

Consent can either be in written, recorded, and/or in electronic form. It must be signed by the patient, guardian, or authorized representative, in accordance with this code. If a patient is incapable of affixing his or her signature, a finger print, thumb mark, electronic signature, or other biometrics may be considered, provided that a witness of legal age and sound mind is present.

1.7. *Revocation and Reinstating Consent.*

Where consent was previously given by an authorized representative on behalf of an unconscious or otherwise incapacitated patient, such consent may be subsequently revoked by the latter once he or she recovers consciousness or regains the capacity to give consent.

1.8. *Exemptions for Consent.*

Consent shall not be required for the processing of personal data in the PHIE under the following conditions:

(a) For purpose of medical treatment, carried out by a medical practitioner or a medical treatment institution;
(b) When necessary to protect the life and health of the patient or another person, and the patient is not legally or physically able to express his or her consent prior to the processing;
(c) When processing is requires by existing law and regulation, such as, but not limited to:
    (1) Act 3573: law of reporting of communicable diseases;
    (2) Administrative Order No. 2008-0009: Adopting the 2008 revised list of notifiable diseases, syndromes, health-related events and conditions.

2. *Point of Collection of Information.*

Collection of information shall start at the time of registration in the health facility and shall be carried out in the admitting or registration section. Subsequent collection of information shall be undertaken at different points of the care provided to the patient.

3. *Processing of Information.*

Processing of Health Information may be through an Electronic Medical Record (EMR) system or Health Facility Information System for service transactions within the coverage and capability of the Health Facility Information System. If the health facility does not have an EMR system in place, encoding and processing of patient information will be coordinated through the medical records section or health facility information management section.

4. *Patient Identifier.*
A patient's unique identifier shall be his or her PhilHealth Personal Identification Number.

5. *Point of de-identification.*
Only de-identified health information shall be stored in the PHIE Data Warehouse. De-identification shall be performed upon contact with the Participating Health Care Provider (PHCP). The PHCP shall transmit information from patients' records to PHIE as shared health record or as part of PHIE's data warehouse. If the patient consents, the patient's health record, or as part of the PHIE as a shared health record, or as part of the PHIE's health data warehouse.

Where the consent of a patient has been obtained, his or her health record may be processed in the PHIE without the need for de-identification. Otherwise, health information must be de-identified, leaving only those information necessary for immediate statistical reference.

6. *Highly Communicable Disease and Special Conditions.*
For patients with special conditions and/or highly communicable diseases such as, but not limited to, HIV, Ebola, MERS-COV, special codes shall be given. Additional documents shall also be signed by the patient, attending physician and head of the facility.

7. *Authorized personnel to amend data if required.*
Data collection and processing shall be done by an authorized employee of the health facility and shall ensure that Clinical Practice Guidelines are observed when changing data, specifically:

A. original entry must be visible;
B. change must be dated and countersigned, or logged; and
C. reason for the change must be entered or specified.

The medical social worker or some equivalent personnel shall collect information, especially salient points such as family information, socio-economic profile, and other vital data.

8. *Reportorial Requirements.*
In compliance with Act No. 3573 also known as the "Law on Reporting of Communicable Diseases", all notifiable diseases, syndromes, events and conditions shall be immediately collected and reported to the local and national authorities.

Conforming to Executive Order No. 292 (s.1987), relevant information on the country's health situation shall be collected, analyzed and disseminated by appropriate authorities provided that health information of patients shall be protected and shall statistical data shall only be provided.

9. *Information to be Shared.*

PHCPs shall share health information exclusively for continuity of medical services. Health information shall be retained and shared only for purposes prescribed upon its collection.

10. ***Filing and Storage***

A. All information collected at different levels of care shall be integrated into a common file. An electronic archiving system shall be developed for the storage of electronic data.
B. Health care providers shifting to electronic records shall ensure that their paper records are stored properly. Paper records shall be digitized for the purpose of preservation and not destruction.
C. Subject to existing regulations, all medical records, whether in electronic and/or paper format, shall be stored for fifteen (15) years. For medico-legal cases, records shall be stored for a lifetime.
D. Providers of electronic medical records shall have a filing and storage protocol.

Rule 2
Access of Health Information

1. ***Access of Health Care Providers.***

Upon patient consent, only a health care provider and authorized entities as defined in Article IV, Section 1, shall have access to the patient's health information.

1.1. ***Accessible Information for Health Care Providers.***

For healthcare providers, accessible information shall consist of the following:

a. History of past illness;
b. Family history of illness;
c. History of present illness;
d. Clinical history, including immunization records, previous operations and treatment;
e. Allergies;
f. Medication history including adverse effects, if any;
g. Results of laboratory and diagnostic procedures;
h. Treatment outcome (Final diagnoses shall be included whether clinical or confirmed).

1.2. ***Approval of Access.***

The creation of user credentials for personnel that shall have access to electronic medical records must be requested based on the recommendation of the head of the medical record section or unit of a health facility and subject to the approval of the head of the facility.

2. ***Access of Patient or Client.***

Consenting patients or clients shall have rights to access on how their health information is used. The health facility shall ensure that disclosures and any subsequent changes are in accordance with the law and are properly documented.

2.1. ***For Minors.***
Either parent or a legal guardian shall have access to the child's health information. Where legal custody has been granted to only one parent or where the child has no parent, only the parent with legal custody or the person appointed by the court as legal guardian of the minor shall be allowed access to the records.

2.2. ***For the incapacitated.***
Where the person requesting access to the health information is incapacitated, a person in whose favor a special power of attorney has been executed shall be allowed access to the records.

3. ***Access of Third Party.***
Any third party will be allowed access to health information of a patient in cases required by law, or when such access is authorized under a valid contract to which the patient is a party.

3.1. ***Third Party Use and Disclosure.***
A third party shall not disclose health information unless provided in a contract or required by law. It shall use appropriate safeguards to prevent use and disclosure of the health information other than as provided by contract or as required by law.

Such third party shall report to the health care provider any unauthorized use or disclosure of health information it becomes aware of, including personal data and security incidents.

Rule III
Use and Disclosure of Health Information

1. ***Use and Disclosure.***
Use and disclosure of health information shall be limited to that covered by the consent given by the patient, or his or her authorized representative, and shall only be for the following purposes:

A. Planning of quality services;
B. Reporting of communicable, infectious and other notifiable diseases, including those that pose a serious health and safety threat to the public such as, but not limited to:
    a. Meningitis;
    b. Food Poisoning (Mass);
    c. Breakthrough epidemic of contagious disease;

d. Biological or chemical warfare;
e. Emerging and re-emerging diseases;

C. Continuing care to patients;
D. Reporting of physical injury;
E. Reporting of interpersonal violence to proper authorities;
F. Reporting of diseases as registered in the Philippine Integrated Diseases Surveillance and Response;
G. Mandatory reporting required by licensing and accreditation bodies (e.g., Department of Health, Philippine Health Insurance Corporation, Department of Interior and Local Government, Department of Social Welfare and Development, etc.).

1.1. *Deceased Individuals.*
Disclosure of health information of a deceased individual shall be made to the authorized representative.

1.2. *Medico-legal cases.*
In medico-legal cases, information may be disclosed to the authorized personnel in-charge upon authorization from the patient or authorized representative (in case the patient is deceased).

1.3. *Legal Authorities and/or Government Agencies.*
Disclosure of health information to any other government agency may only be allowed pursuant to a lawful order of a court. However, in case of emergency, where time is of the essence, disclosure may be made even without court order. This would refer to situations such as:

(a) Where access is sought by virtue of a subpoena. Consent is not required from next of kin;
(b) For medical or financial assistance requesting abstracts or similar documents, authorization of patient is required;
(c) For DOH programs and other government agencies providing financial public assistance the said agency shall only disclose de-identified information.

Without a court order, release of information shall be pursuant to hospital policy otherwise, patient records shall not be released or disclosed.

When personal health information is released to a legal authority, a cover letter shall be sent to the latter emphasizing that health information must be handled in a confidential manner. A receiving copy shall be maintained by the health care provider for record purposes.

2. *Privilege Communication.*

Where information qualifies as privileged communication, as defined in this Code, both the consent of both the patient and physician must be secured prior to the use and/or disclosure of patient information for whatever purpose.

3. *Training Hospitals and Academic or Clinical Requirements Purposes.*
PHCP's shall draft guidelines for the retrieval of information necessary for complying with the requirements of the Professional Regulation Commission (PRC).
A nondisclosure clause shall be included in the contract of a school affiliated with a PHCP. Personnel and/or students of such a school that access data in the custody of the PHCP for academic or clinical requirement purposes shall also sign a nondisclosure agreement.

RULE 4
Organizational Security Measures

1. *Policies and Procedures.*
Each health facility shall create its own privacy protocol. Privacy and security policies must be documented, maintained and updated as appropriate.

1.1 The PHCP shall develop policies and establish procedures that specify the groups and positions that require access to health information in order to perform their functions and responsibilities, as well as the type of health information to which they need access.

1.2 PHCPs shall orient their employees and other personnel, particularly those involved in information security, regarding their respective privacy and security policies.

1.3 PHCPs shall clearly define access rights and user roles among their employees and other personnel to ensure that only those people with the requisite authorization are able to access protected health information.

1.4 For this purpose, the Chief of each PHCP shall issue a memorandum containing a list of its authorized personnel, and thereafter furnish the DOH central office a copy thereof.

1.5 Each PHCP shall perform a regular privacy and security audit.

2. *Contract with Third Party.*
Contracts or agreements between a PHCP and a third party shall include:

A. policies for document storage and disposal;

B. data management process, including methods for tracking and controlling records (e.g., dates and time stamps), the type of data sent and received, and the individuals who have access to records;
C. description of the privacy and security programs of the third party;
D. description of output reporting (e.g., electronically or in hard copy) that allows for the viewing, monitoring, and/or reconciling of data;
E. periodic staff training in secure records-handling, and -providing, and appropriate document management tools;
F. staff responsibilities for ensuring compliance and allocation of sufficient job time to the task; and
G. communication requirements regarding control deficiencies identified through internal or external sources.

3. *Authorization and Document Retention.*
For identification and authorization purposes, the authorizing entity shall provide any of the following:

A. biometrics
B. specimen signature
C. e-signature

The document retention policy issued by the National Archives of the Philippines shall be followed. For archiving purposes, a PHCP can maintain an internal archiving system or outsource such task to an archiving specialist.

4. *The Information Technology Personnel.*
Authorized personnel responsible for supporting the implementation of security guidelines must adhere to the policy of confidentiality of medical records. They shall also be charged with the conduct of system-related functions such as, but not limited to, troubleshooting.

5. *The Medical Records Officer.*
The Medical Records Officer with the Privacy Officer has the authority to audit the patient's shared health record of patients.

Rule 5
Physical Security

1. *Inventory of Information Technology Physical Devices.*

The Information Technology (IT) personnel of a PHCP shall maintain and update an inventory of all IT physical devices being used in the facility. The inventory shall include, but not be limited to, on-premise server equipment, firewall and security devices, client workstations, network devices, mobile devices, biometric and authentication devices, as well as other present and future IT devices that may be relevant to the purposes of PHIE.

2. ***Access to Physical Infrastructure.***

A health facility shall define the access system to its I.T. physical infrastructure and limit the same to authorized personnel only. Any special access to such infrastructure shall be documented thoroughly. Any unauthorized access shall also be documented and escalated to the appropriate decision-maker for further investigation and action.

2.1. ***Server Access.***

A health facility may opt to have either an on-premise server, a cloud server environment, or a combination of the two. Should it choose to maintain an on-premise server, it shall provide a designated area (i.e., server room) for the housing of servers or data centers. The area must be separated from the site for data collection and processing, and from the office of the IT personnel. It must also comply with the physical security ISO 27001 standards.

Cloud technology is discussed separately under the cloud services section of this document.

2.2. ***Computer Access.***

Pre-deployment site assessment shall be conducted prior to installation of computer workstations in the health facility. Computers shall be accessible to authorized personnel, in accordance with a role-based system access. Each user shall only have one account. A person requesting access to a computer shall fill-out the prescribed request form.

Anti-glare filters on computer monitors shall be installed. Apart from reducing glare, they also provide additional security by preventing, or at least minimizing, unauthorized and/or accidental viewing of the computer screen.

2.3. ***Computer Loss.***

In case of computer loss, the accounts in the computer system shall be reset and deactivated until it is retrieved or reported. The Data Protection Officer shall implement security incident procedures and contingency plans for such events.

3. ***Bringing of devices outside the health facility.***

Devices registered with the health facility shall not be brought outside its premises, unless the point of patient encounter is outside the health facility, such as but not limited to the following scenarios: vaccinations, remote visits, and other similar or related community-oriented activities

undertaken outside the health facility. Where devices are brought outside, proper documentation and security checks must be carried out. As a required minimum, the following security measures should be in place:

A. Hard disk encryption
B. Data encryption
C. Wireless network
D. Role-based access control
E. Anti-virus software for vulnerable operating systems
F. Password-protected user access that complies with facility password policies of the health facilities.
G. Encrypted portable devices such as, but not limited to, Flash Drives, secure digital (SD) card drives, rewritable compact discs (CDs), and other present and future devices.

4. *Bring-your-own device (BYOD).*

Mobile and portable devices owned by the health facility personnel may be allowed by the health facility, provided that the latter shall implement strict policies for the access, processing, storage, transmission and output of data, given their possible implications on patient privacy and health information security.

4.1. *Agreement.*

Prior to the use of a BYOD in the handling of health data and information, its owner must submit a signed usage agreement.

4.2. *Training.*

BYOD users shall undergo annual security training.

4.3. *Configuration.*

The IT personnel of the health facility shall establish a mechanism that creates an audit trail of the system activity by the BYOD user, including log-in attempts, security incidents, and attempts to access files containing personally identifiable information. The mechanism shall also have a provision for remote access by the IT personnel, in such events that privacy of health data and information are compromised.

4.4. *Device Requirements.*

Before a BYOD is certified as being allowed for use when accessing health information, the privacy officer shall first approve a checklist of requirements, which shall, as a minimum, require that the device have the following:

a. hard disk encryption.
b. data encryption

c. wireless network encryption
d. role-based access control
e. anti-virus software for vulnerable operating systems.
f. password-protected user access that complies with facility password policies.
g. encrypted portable devices such as but not limited to flash drives, secure digital (SD) card drives, rewritable CD, and other present and future devices.

Mobile devices used for job responsibilities are subject to audits even if owned by an employee of the health facility.

Taking photos of patient data through the use of camera phones and bringing of unauthorized electronic devices such as cellular phones, laptops, tablets, and cameras inside the medical records area is prohibited.

5. *Business continuity and Disaster recovery.*
The health facility shall implement policies for business continuity and disaster recovery.

5.1. *Physical backup.*
A data backup plan has to be implemented to create and maintain exact copies of the system for handling health information. The backup medium must be defined, and the interval of backup stated. The backup must also be tested for data validity and integrity. Physical backups shall be encrypted and stored outside the health facility and additional physical security measures shall be in place for accessing and securing the physical backups. In the event of a disaster, the Data Protection Officer must have a protocol in place for data recovery and a disaster recovery team that can be organized within a short period of time.

5.2. *Business Continuity.*
Business continuity must be ensured even in the event of a disaster. The Data Protection Officer shall have identified a minimum set of data requirements for the maintenance of the processes of a health facility necessary for the delivery of services. The health facility shall also have the ability to transition from "emergency-mode" services, to full services. For this purpose, policies for encoding data outside the "full services" mode must be in place.

Events that take place during disaster recovery and business continuity shall be documented and reviewed. Updates implemented according to best practices and lessons learned during the disaster period.

Rule 6
Technical Safeguards

1. *Access Controls.*

Technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to persons or software programs that have been granted access rights:

1.1. *Information Access Management* *(Required).*

(a) Isolating health care clearinghouse functions (Required). If a healthcare clearinghouse is part of a larger organization, the clearinghouse shall implement policies and procedures that protect the electronic protected health information from unauthorized access by a larger organization.

(b) Access authorization (Addressable). Policies and procedures for granting access to electronic health information, such as those that relate to workstation access, transaction, program, process, and/or other mechanisms shall be implemented by the PHCP. Guidelines on the access to health information are provided on Article III of this Code.

(c) Access establishment and modification (Addressable). Policies and procedures of an establishment, including those that relate to the documentation, review and modification of a user's rights to workstation access, transaction, program or process shall be implemented based on the access authorization policy of the data controller and/or data processor.

1.2. *User Identification* *(Required).*

A process for unique user identification shall be made within the policy and procedure of the PHCP.

A. There shall be a user name and/or number for identifying user identity throughout all levels of the organization.
B. User identity shall not be shared, delegated or assigned to a group or individual.
C. User identity that was previously used shall not be reused for new and/or existing users.

1.3. *Emergency Access Procedure* *(Required).*

Procedures for obtaining necessary electronic health information during an emergency.

(a) The PHCP shall identify, define, and describe the situations when emergency access to health information may be authorized.
(b) Personnel who are authorized to access health information during emergency situations must be identified.

(c) Procedures for obtaining necessary health information during emergency situations shall be established and implemented.
(d) Policies and procedures for governing access to health information shall be established.

1.4. *Automatic Log-off* *(Addressable).*

Electronic procedures that terminate and electronic session after a predetermined time of inactivity.

(a) A policy and procedure regarding the use of automatic log-off shall be created.
(b) A predetermined time shall be documented within the policy based on the application.

1.5. *Encryption and Decryption* *(Addressable).*

The method of converting an original message of regular text into encoded text using an algorithm.

A. For encryption in transit, the standard security technology shall be SSL (Secure Sockets Layer).
B. Minimum standard requirement for encryption shall be AES (Advanced Encryption Standard) 128.
C. For encryption in storage, the standard shall be TKE (Trusted Key Entry).

1.6. *Multi-factor Authentication* *(Addressable).*

For systems that have been identified as having significant risks (e.g. servers, unified threat management), policy, operational, and technical mechanisms that use multi-factor authentication shall be put in place.

2. *Audit Controls.*

Relative to a particular computer system, there shall be a record of those who have access thereto, when it was accessed and what operations were performed.

2.1. *Recording of Information* *(Required).*

Recorded information must include, but is not limited to, unique user identified, data and time of use/access, location (if applicable).

2.2. *Audit Data Life Span* *(Addressable).*

The PHCP shall establish a policy that specifies the period within which data must be stored, and the method for its destruction or disposal.

2.3 *Access to Audit Data* *(Addressable).*

The Medical Records Officer alongside with the Data Protection Officer shall be authorized to audit the shared health record.

3. *Integrity Controls.*
Protection of Health Information from improper alteration or destruction.

3.1. *Mechanism to Authenticate Electronic Health Information* *(Addressable).*
There shall be a mechanism in place that confirms that electronic health information has not been altered or destroyed in an unauthorized manner.

3.2. *Digital Signatures* *(Required).*
Digital signatures shall be used to verify the authenticity of the entry in an electronic system.

3.3. *Sum Verification* *(Required).*
Sum verification shall be used to determine if the input data matches source data.

3.4. *Anti-virus Software* *(Required).*
Computers shall have an industry-standard anti-virus software with its automatic update feature turned on. The software shall be configured regularly and shall automatically download updates to ensure its ability to address the latest threats.

3.5. *Data Storage Encryption* *(Required).*
Data storage and transmission shall be encrypted. For websites, https encryption shall be used. Article VII, section 1.5 provides standards for encryption and decryption.

3.6. *Transmission Encryption* *(Required).*
Data transmission via wireless networks or the internet shall always be encrypted.

3.7. *Proper Handling of Mechanical Components* *(Addressable).*
Users of electronic systems shall be trained on the proper use and handling of central processing units (CPUs), servers, flash drives, and external hard drives.

3.8. *Offline Modes and Caching* *(Addressable).*
Electronic systems shall have online and offline modes.

3.9. *Interface Integration of Information Systems* *(Addressable).*
Data transmission from electronic medical records shall follow a standard for integration and interfacing in order to facilitate interoperability and data compatibility.

4. *Transmission Security.*

Technical security measures to guard against unauthorized access to electronic health information that is being transmitted over an electronic communications network shall be implemented.

5. *Identity Authentication.*
Procedures necessary to verify the identity of a person or entity seeking access to electronic health information is the one claimed shall be implemented.

6. *Storage Security.*
Data stored in a portable data storage device (e.g. flash drive, portable hard drives, etc.) and/or in cloud storage services (e.g. Dropbox, OneDrive, Google Drive, etc.) must be encrypted.

Rule 7
Cloud Services

1. *Cloud Services.*
Where applicable, a PHCP must familiarize itself with the technologies being used by its cloud serviced provider in delivering its services, including the implications that technical controls have on the security and privacy of the system throughout its lifecycle.

For cloud service providers, there shall be in place:

1.1 appropriate audit mechanisms and tools capable of determining how data is stored, protected, and used, and of validating services and policy enforcement;
1.2 a risk management program that is flexible enough to deal with the continuously evolving and shifting risk landscape; and
1.3 adequate and secure network communications infrastructure.

The cloud service provider's electronic discovery capabilities and processes must not compromise the privacy or security of the data and applications of the PHCPs. At the same time, the PHCP must also be familiar with the cloud service provider's security measures in order for it to conduct proper risk management.

The PHCP should understand the privacy and security controls of the cloud service. It must establish adequate arrangements in the service agreement that allow for necessary adjustments and effective compliance monitoring of said controls with the terms of the service agreement.

2. *Contract between health care provider and cloud service provider.*

2.1 The health facility's ownership rights over the data must be firmly established in its service contract with the cloud service provider should clearly state that:

A. The healthcare provider retains ownership over all its data;
B. The cloud service provider acquires no rights or licenses from the agreement, including intellectual property rights or licenses to use the health care provider's data for its own purposes; and
C. The cloud service provider does not acquire and may not claim any interest in the data.

2.2 Service agreements should also:

A. Provide means through which a PHCP can assess the performance of the cloud service provider over time, including the security controls and processes it employs. Whenever possible, the PHCP shall have such information (e.g., threshold for alerts and notifications, level of detail and schedule of reports, etc.) that is proportionate to its needs.

B. Clarify the types of metadata collected by the cloud service provider, the protection provided thereon, and the organization's rights over metadata including ownership, opting out of collection or distribution and fair use.

3. *Composite Services.*

Where cloud services themselves use third-party service providers as regards one or more of their services, they should specify the scope of control of the third parties, their responsibilities, and the remedies and recourse available in case problems occur. These arrangements shall, in all cases, comply with the requirements set out in the DPA regarding the outsourcing or subcontracting of data processing.

Rule 8
Use of Social Media

1. *Definition of Social media.*

This refers to electronic communication, websites or applications through which users connect, interact or share information or other content with other individuals, collectively form part of an online community. This includes such online platforms as Facebook, Twitter, Google+, Instagram, LinkedIn, Pinterest, Blogs, Social Networking Sites.

2. Unauthorized posting of personal data of patients in social media, including pictures, shall be penalized in accordance with the provisions of the DPA.

3. *Administrative Responsibilities.*

Health facilities shall provide for guidelines regarding the use of social media. In line with this, the social media activity of all facility personnel, whether temporary or permanent, shall be

monitored for any privacy breaches. For this purpose, "facility personnel" shall include: (a) physicians; (b) employees; (c) other healthcare providers; (d) students; (e) and residents in training, practicing their profession, working, or fulfilling academic and clinical requirements within the health facility.

Unprofessional behavior or misinformation witnessed in social media that violates patient privacy or privacy of other individuals shall be reported to appropriate authorities.

4. *Responsible Social Media Use of Health Care Professionals.*
Health care professionals shall always be mindful of their duties to their patients, community, their profession and their colleagues thus they must take into account that any content, once posted online, may be easily disseminated to others and is essentially irreversible.

5. *Health Education and Promotion.*
Caution must be observed when sharing health-related information, education, and promotion for advocacy purposes.

Only general opinions may be shared in social media. Specific medical diagnosis, advice, treatment or projection shall not be dispensed with therein. Accordingly, social media use, whenever appropriate, shall always include statements reminding the public that they should not rely on advice given online, and that medical concerns are best addressed in the appropriate settings.

For social media use to crowd source support, identity of the patient can only be revealed to the support group upon patient's consent. Confidentiality of data shall still be upheld by removing any information or features that are easily identifiable to the patient.

6. *Professional Guidelines for Social media Use for Persons Involved in the PHIE.*
A health care professional shall:

6.1 strive to develop, support and maintain a privacy culture in the health facility. He or she shall abide by the social media use policy of the facility.

6.2 advise the patients of their privacy rights and encourage them not to post in social media any activity or confidential information that may put them at risk, such as, but not limited to medical diagnosis and laboratory results.

6.3 conduct himself or herself in social media or online the same way that he or she would in person for this purpose, he or she shall act in a manner befitting his or her profession, thereby inspiring trust in the service he or she provides. This is particularly the case if said

professional maintains the same social media account for both his professional and personal lives.

6.4 refrain from using the name, log, or any other symbol of the health facility in his or her social media activity, without proper authorization. An individual shall also not identify himself or herself in social media as a representative of the facility absent any authority to do so.

6.5 refrain from posting, sharing, or using photos or videos taken within the facility that will violate their right to privacy.

Rule 9
Human Resources

1. *On-boarding of employees of the health care facilities.*
All candidates for employment, contractors and third parties shall be screened properly by the concerned personnel of the health facility, particularly those being considered for sensitive posts.

As part of his or her security roles and responsibilities, an individual shall:

A. implement and comply with the health facility's information security policies;
B. protect assets from unauthorized access, disclosure, modification, destruction or interference;
C. execute security processes of specific activities;
D. ensure responsibility is assigned to an individual for actions taken; and
E. report security events or potential events or other security risks to the organization.

These functions shall be clearly defined and communicated to the personnel concerned.

Background verification checks on all candidates for employment, contractors, and third parties shall be carried out in accordance with relevant laws, regulations and ethics, and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Procedures shall define criteria and limitations (e.g., who is eligible to conduct screening, manner by which screening shall be carried out, etc.) for verification checks.

A screening process shall be carried out for contractors, and third parties. In the case of personnel of third parties processing health information for or in behalf of a health facility, or where the services of contractors are secured by such facility through an agency, the contract with the third party or agency shall clearly specify the latter's responsibilities vis-à-vis the

screening process as well as the notification procedure it needs to follow if screening is not completed or if the results thereof give cause for doubt or concern. In the same way, the agreement with the third party should clearly specify all responsibilities and notification procedures for screening.

Personnel of the health facility, the latter's contractors, and third parties processing health information for the facility, shall agree to and sign the terms and conditions of their employment contracts. Such terms and condition must reflect the health facility's security policy, and shall clarify the following:

A. All personnel of the facility, its contractors, and third parties processing health information for the facility, who are given access to personal data shall sign a confidentiality or non-disclosure agreement prior to being given such access;
B. Rights and responsibilities (e.g., copyright laws or data protection legislation) of all personnel involved;
C. Responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by all personnel involved, contractor or third party user;
D. Responsibilities of each personnel as regards the handling of personal data received from other companies or external parties;
E. Responsibilities of the organization for the handling of personal data, including that created as a result of, or in the course of, a person's work in the organization;
F. Responsibilities that are extended outside the organization's premises and outside regular working hours;
G. Actions to be taken if the organization's security requirements are disregarded by a specific individual.

2. *Employment Period.*

No personnel shall disclose any personal data relating to a patient without the latter's consent. This prohibition shall subsist even after such personnel's employment or engagement with the health facility.

2.1. *Management Responsibilities.*

Management responsibilities should be properly defined to ensure that security is applied all throughout an individual's employment or engagement with the health facility.

Management responsibilities shall ensure that personnel of the facility, including those of its contractors and other third parties:

a. are properly briefed regarding their information security roles and responsibilities prior to being given access to sensitive personal information or information systems;

b. are provided with guidelines that identify the security expectations from their respective roles and responsibilities;
c. are motivated to fulfill the security policies of the health facility;
d. achieve a significant level of awareness regarding information security that is relevant to their roles and responsibilities;
e. conform to the terms and conditions of their employment or engagement, which includes the health facility's information security policy and appropriate methods for working; and
f. have the skills and qualifications necessary for the fulfilment of their respective roles and responsibilities.

2.2. *Awareness and Training.*

An adequate level of awareness, education, and training in security procedures and the correct use of data processing facilities should be provided to all personnel of a health facility, including those of its contractors and other third parties it conducts business with. A formal disciplinary process for handling security breaches must also be established.

Awareness training shall commence with a formal induction process designed to introduce the health facility's security policies and expectations before access to data or services is granted to the concerned personnel.

The security awareness, education, and training activities should be suitable and relevant to the person's role, responsibilities and skills, and should include information on known threats, who to contact for further security advice and the proper channels for reporting personal data breaches and security incidents.

2.3. *Disciplinary Process.*

There shall be a formal disciplinary process for personnel charged with having committed a personal data breach or security incident, or, by the negligence, allowed such breach or incident to occur.

For this purpose, a health facility shall accord due process to the personnel involved.

For government-owned health facilities, any disciplinary or termination process shall be in accordance with the Civil Service Rules.

Regarding administrative liability, a graduated response that takes into consideration various factors (i.e., nature and gravity of breach and its impact on business, whether or not it is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts, etc.) shall be provided.

3. *Termination or Off-boarding of Employees.*

Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned. Responsibilities and duties still valid after termination of employment shall be contained in the employee's, contractor, or third party's contracts.

The communication of termination shall include ongoing security requirements and legal responsibilities contained within any confidentiality agreement, and the terms and conditions of employment continuing for a defined period after the end of the employee's, contractor or third party's engagement.

The Human Resources function is generally for the overall termination process and works together with the supervising manager of the person leaving, the IT manager to manage the security aspects of the relevant procedures in relation to health information access. In the case of a contractor, the termination responsibility process may be undertaken by an agency responsible for the contractor, or be handled by their organization.

3.1. *Return of Assets.*

All employees, contractors and third parties shall return all of the health care facility's assets in their possession upon termination of their employment, contract or agreement.

The termination process shall be formalized to include the return of all previously issued software, corporate documents, and equipment. Other organizational assets such as mobile computing devices, access cards, software, manuals, and information stored on electronic media must also be returned.

In cases where an employee, contractor or third party has information that is important to ongoing operation, such information shall be documented and relayed to the organization.

3.2. *Access Rights.*

The access rights of all employees, contractors and third parties to data and data processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

If a departing employee, contractor or third party is in possession of passwords to accounts that will remain active; these shall be changed upon termination or change of employment, contract or agreement.

Access rights to data assets and data processing facilities shall be limited or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

a. whether the termination or change is initiated by the employee, contractor or third party, or by management, and the reason for termination;
b. current responsibilities of the employee, contractor, or any other user;
c. value of the assets currently accessible.

In certain circumstances access rights may be allocated on the bases of being available to more people than the departing employee, contractor or third party (e.g. group IDs). In such instances, departing individuals shall be removed from any group access list and arrangements shall be made to advice other employees, contractors and third parties involved to no longer share this information with the person departing.

Rule 10
Health Research

1. *Research Subject.*
Research participant shall be made to understand that he or she can opt-out of the study or have his or her personal data deleted from the project's database if they relay such request in writing.

A. *Acceptable recruitment methods.* Acceptable methods for recruiting research subjects may include: advertisements, notices, media (social or tri-media), websites, letter or email to colleagues or healthcare staff that may be distributed to potentially eligible individuals.

B. *Unacceptable recruitment methods.* Unacceptable recruitment methods for recruiting research subjects include: (1) searching through medical records or databases (e.g., patient registry) for qualified subjects and having a researcher with no prior contact with potential subject recruit; (2) recruiting subjects immediately prior to sensitive or invasive procedure (e.g. in pre-op room); (3) retaining sensitive personal information obtained during screening without the consent of those who either failed to qualify or refused to participate in any possible future study.

2. *Research Protocol.*
Study protocols shall incorporate data protection measures. Protocols shall describe how the participant's privacy will be protected in the entire research process and shall also include provisions on how to protect data and samples during use and subsequent storage.

A letter of request addressed to the Local Chief Executive or the Head of the Facility shall be made and shall be subject for approval. The letter of request shall contain the objective of the study, the type of data to be collected, and the method of data gathering.

Individuals, organizations or third parties who may access health information shall be identified in the study protocol and in the registration information to be provided to the concerned review body.

3. *Research Projects.*
A research project involving one thousand (1,000) or more data subjects shall register with the National Privacy Commission and/or its duly deputized body (for health research, possibly the Health Privacy Board).

A personal data breach reporting protocol shall be followed and researchers must ensure data protection during the entire research process (e.g., recruitment, study proper, close-out, etc.) and, where applicable, even after the conduct of study.

All personnel involved in the study will be required to sign agreements to protect the privacy, security and confidentiality of the health information before they are granted access to any personal data or research participant.

A copy of the completed research study or project shall be provided to the health facility.

4. *Research Data.*
Data or specimen collected from research shall be de-identified or destroyed only when deemed appropriate. Identifiers will be removed from study-related information, whenever feasible.

A. *Paper-based records.* Paper-based records are to be kept in a secure location and shall only be made accessible to personnel involved in the study.

B. *Electronic records.* Computer-based files will be encrypted and made available to personnel involved in the study through the use of access privileges and passwords.

C. *Audio and video collection.* Audio or video recording of research participants will be transcribed and thereafter destroyed to eliminate audible or visual identification. Collection of visual images shall be subject to patient's consent and identification of data. Collection of visual images shall be subject to patient's consent and identifiable information shall be removed or obscured.

D. *Data Sharing.* Where the health information of a research participant shall be subject to a data sharing arrangement, his or her consent must be obtained specifically for such purpose. Data sets that will be disclosed to the public must have undergone thorough technical anonymization procedures and shall have been cleared for public access by a

duly-constituted ethics committee. The risk of re-identification of study participants or data subjects should be low to none.

Rule 11
Patient Registries

1. *Registry Design.*
Any give registry shall be developed with a clearly-defined purpose (i.e., disease condition, health service registry, disease outcome, etc.) to avoid both ethical and compliance issues that may undermine the attainment of such purpose.

A governance framework for registries shall be formalized to: (a) ensure accountability; (b) oversee resource application; (c) provide focus; and (d) optimize output from said registries. All personnel involved in the use of these registries must be familiar and abide with the administrative and legal requirements set out in such framework.

Methods involved in the registry such as but not limited to data collection, data reporting, and addressing of outliers shall be documented.

A security assessment approach shall be employed to identify measures that need to be adopted to address security gaps.

2. *Informed Consent.*
Health facilities shall declare the patient registries that they are managing. Registry participants or their next of kin shall be made aware of the collection of data for the use of or storage in such registries.

3. *Registry Data.*
Data elements shall conform to standard definitions, terminologies and specifications. It must be used to enable meaningful comparisons and allow maximum benefit to be gained from linkage to other registries and/or databases. Registry reports shall be produced according to a strict timeline.

Data dictionaries shall be established to ensure that a systematic identical approach is taken during data collection and data entry.

For data previously collected, the privacy conditions under which they were collected shall be set as the minimum privacy conditions.

Audit of registry data shall be done frequently (depending on facility protocol) to promptly identify data quality lapses.

4. *Data Collection.*
Collection of data shall be done as close as possible to the time and place of care by appropriately trained data collectors. It shall be done in a systematic approach, with identical approaches used at different institutions ensuring that it shall not be an unreasonable burden to patients, nor incur any cost.

5. *Registry Data for Research.*
Health information registries for research shall incorporate an appropriate design and data elements, written operating procedures, and documented methodologies, as necessary, to ensure the fulfillment of a valid scientific purpose.

Where an authorization for the use and disclosure of registry data for future research does not exist, health care provider or health insurance plan maintaining the registry shall need to obtain additional authorization for the research from individuals or seek a waiver of authorization from an Institutional Review Board, Ethics Review Board or Health Privacy Board.

6. *Registries for Vulnerable Population.*
Registries compiling health information from vulnerable population such as but not limited to pregnant women, human fetuses, neonates, prisoners, children, and patient having rare diseases shall employ special effort to protect identities of these subjects.

7. *Linking of Registries.*
If a dataset is going to be linked to another, an independent review of privacy risks (i.e re-identification, fraud) involved must be conducted.

Rule 12
Publication and Public Communication

1. *Publication of Privacy Policy.*
Privacy protocols of health facilities shall be available both in written and electronic forms and shall be distributed to all employees.

Health facilities shall ensure that appropriate signage indicating the availability of protocols are posted. Privacy protocols of health facilities shall be updated and submitted to the Health Privacy Board and in so far as practicable, be made available online in its own website.

2. *Site Privacy Policy.*

A. For facilities maintaining public-facing websites:

a. Any information that may compromise the privacy of the patient shall not be posted in the website.
b. Any data collected by the website shall be treated with utmost confidentiality.
c. Where applicable, the health facility operating the website shall declare that it uses cookies to manage authentication, navigation, and other functions. It shall also actively request a site user to agree that these types of cookies can be placed on one's device.

Rule 13
Health Privacy Board

1. *Rationale.*

The Health Privacy Board is a broad sectoral response to health information privacy needs. It will support the health sector in complying with issuance and administrative orders relating the health information privacy and further the development of policy and practice for health data protection.

2. *Composition.*

The Health Privacy Board shall be composed of the Chairperson who shall be assisted by two Board Members, one to be responsible for Training and Capacity Building and one to be responsible for Compliance and Planning.

2.1. Appointment of full-time Board Members with salary grade not lower than 26 shall be done by the Steering Committee of PHIE. They shall be provided with office and administrative staff.

3. *Competencies and Qualifications.*

Members of the Board shall have the following competencies and qualifications:

a) Background in law, education, clinical or public health, a bachelor's degree in management, information systems, human resources, health administration, or other relevant fields.
b) Minimum 5 years' experience in health care.
c) Demonstrate mastery of regulatory development and compliance, including standards, laws and regulations concerning information security and privacy.

d) Familiar with business functions and operation of large institutions (preferably health-related).
e) Strong organizational and problem-solving skills.
f) Work effectively with teams and stakeholders.
g) Have the ability to communicate with clarity both orally and in writing.

4. *General Roles and Functions*.

1. The Board shall assist in the implementation of the Privacy Guidelines and related issuance through Training and Capacity Building, and through Compliance Monitoring and Planning.
2. It shall coordinate with the licensing authority of the heath institution or other accreditation bodies, when necessary, in order to perform its function.
3. The Board shall accept complaints, inquiries and requests for assistance from the health sector on matters related to the Privacy Guidelines and related issuance.
    a. Complaints. It shall promulgate rules and procedures for receiving and processing complaints. It shall mediate between parties to reach a compromise settlement, without prejudice to reporting before the NPC or licensing and regulatory authorities, matters contrary to law, in which case it shall make its recommendation after proper evaluation.
    b. Inquiries and Requests for Assistance. It shall assist persons or institutions on the interpretation of privacy regulations. It shall elevate to the Privacy Experts Group issues which in its discretion requires advisory assistance.
4. It shall provide the Privacy Experts Group (PEG) a report of its activities, including case reports of issues brought before it that are of importance or significant impact.
5. It shall make recommendations on change in policy or further policy development. It shall coordinate with appropriate agencies to incorporate emerging technologies and new regulations in existing policies.

5. *Board Member for Training and Capacity Building.*

The Training and Capacity Building functions of the Board shall be spearheaded by the Board Member for Training and Capacity Building. He or she shall:

1. Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the health sector.
2. Develop and implement training modules for capacity building.
3. Develop and implement programs to inform and educate the public of health information privacy and to promote a privacy culture in the health sector including but not limited to IEC materials that may be used by health information privacy advocates.

4. Conduct training workshops and accommodate requests for public information on the implementation of the privacy guidelines.

6. *Board Member for Privacy Compliance and Planning.*

The Privacy Compliance and Planning functions of the Board shall be spearheaded by the Board Member for Privacy Compliance and Planning. He or she shall:

1. Oversee the monitoring of privacy compliance in health facilities. It shall develop procedures for assessment of privacy practices in health facilities, in accordance with standards for organizational, physical and technical security measures in the Privacy Guidelines and related issuances. It shall also coordinate with licensing and accreditation bodies to advocate inclusion of privacy standards in their evaluation of health facilities, in view of the requirement of existing laws.
2. Review privacy codes voluntarily adhered to by personal information controllers and processors in the health sector and make recommendations to meet standards for the protection of personal health information.
3. Identify gaps in current standards for organizational, physical and technical security measures for protection of personal health information and make recommendation for its improvement.
4. Develop materials and documents such as templates for employment contracts and non-disclosure agreements to serve as a guide for the health facilities.
5. Undertake regular planning activities to develop and recommend programs to support the implementation of the Privacy Guidelines.
6. Maintain a record of all compliance and monitoring reports.

Rule 14
The Privacy Team of a Health Facility

1. *Rationale*.

In so far as practicable, the Data Protection Officer (DPO) shall be designated at a health facility. The DPO's identity shall be made known to any data subject upon request. It is recommended that the DPO has to be on the Vice-president level (or equivalent) to have sufficient authority to uphold privacy in the institution. Expected to have some personnel with specialized privacy roles are regional health units (RHUs) and bigger health facilities. In a facility where plantilla position for a Data Protection Officer could not be immediately secured, a Privacy-Officer-Designate shall be appointed.

2. *Appointment.*

Hospitals with at least 300 authorized bed capacity shall employ a full time Data Protection Officer. Hospitals with less than 300 authorized bed capacity and other health facilities such as infirmaries, birthing homes, RHUs/BHS, OFW clinics, dialysis clinics, ambulatory-surgical clinic, psychiatric facilities, etc. may federate and designate a shared Data Protection Officer.

The Development Management Officer (DMO) shall be assigned as the Data Protection Officer Designate for Rural Health Units. This shall be in addition to their responsibilities as DMO.

3. *Qualifications.*

The Data Protection Officer shall have the following qualifications:

a) At least a bachelor's degree in management, information systems, human resources, health administration, or other relevant field.
b) Minimum 5 years' experience in health care.
c) Familiar with regulatory development and compliance, including standards, laws and regulations concerning information security and privacy.
d) Familiar with business functions and operation of large institutions (preferably health-related).
e) Strong organizational and problem-solving skills.
f) Work effectively with teams and stakeholders.
g) Have the ability to communicate with clarity both orally and in writing.
h) Must undergo data privacy and security training from reputable training providers.

4. *Roles and Functions.*

Ultimately, the Data Protection Officer is the person responsible for the privacy policy compliance at the health facility. The DPO sees to it that overall compliance is observed at the institution. Other roles of the DPO shall include:

a) Developing and implementing privacy policies and procedures.
b) Assumes advocacy, capacity-building, and stake-holding functions.
c) Manages the privacy aspect in the different areas of the operations.
d) PO and the privacy team shall identify the governance structure from national level down to RHU and align with them their facilities' privacy goals and initiatives.
e) Ascertains the authority and delegates data collection to staff. He or she regularly audits the quality and integrity of patient records.
f) Ensures that the entire process of editing data is documented: request for editing, who did the editing, the process followed in editing, and closing the editing.

g) Identifies how personal health information is created, stored or disclosed in paper and electronic format and maintains an inventory of how we use or disclose all personal health information.
h) Is the contact person responsible for receiving complaints and providing individuals with further information about matters contained in the health facility's privacy protocols.
i) Maintains a record of complaints and brief description of how they were resolved.
j) Distributes the health facility's privacy protocols to all new patients and post the update health facility's privacy protocols on the institution's website or on its public bulletin boards.
k) Continually updates the staff's knowledge of privacy rule guidelines, developments, and new regulations and must train workforce on these requirements. The PO shall update the health facility's privacy protocols, acknowledgement forms, authorization, consents, and other forms as required and ensures that the workforce adheres to the policies and procedures, including imposing sanctions on workforce members that breach an individual's privacy.
l) Effectively communicates technical and legal information to non-technical and non-legal staff for employee training.
m) PO and privacy team shall account for devices used in facility and ensure devices containing electronic personal health information are encrypted as required by health facility's privacy protocols.
n) Reviews all business associate agreements or contracts for privacy compliance.
o) Consistently apply sanctions, in accordance with the facility's policies and procedure.
p) Regularly communicates the status of legal complaints, risk, and sanctions imposed on workforce members.
q) Serve as the practice's resource for regulatory and accrediting bodies on matters relating to privacy and security.
r) Perform system or quality data check, compliance on the reporting forma nd safekeeping of backup data.
s) Coordinate privacy safeguards with the practice's security officer to ensure consistency in development, documentation, and training for security and privacy requirements.
t) Coordinate and communicate to practice leaders and audits of the National Health Privacy Board or any other governmental or accrediting organization.
u) Coordinate with the institution's Risk Manager (if any) to address privacy risks.
v) Reports directly to the hospital director, president, board of directors.
w) Represent the health facility in the event of an inquiry, inspection, or investigation by the National Privacy Commission.

5. *Staff.*

While the DPO is responsible for privacy management and compliance, He or She may delegate responsibilities to others within the organization if they are trained and would communicate promptly with the privacy official on these matters.

Rule 15
Compliance, Incident Reporting, Response

1. *Compliance.*

Health facilities involved in the PHIE are required to:

a. Register their data processing systems involved in the PHIE process to the health privacy board, including the data processing system of contractors, employees and third parties entering into contracts with them that involves accessing or requiring sensitive personal health information from one thousand (1,000) or more individuals;
b. Notify the health privacy board of automatic processing operations being carried out by the health facility, its contractors and third parties;
c. Submit a copy of their privacy policy as well as the list of personnel having direct access to health information to the health privacy board;
d. Submit an annual report on documented security incidents to the health privacy board;
e. Comply with other requirements that may be provided on their issuance issued by the National Privacy Commission or the Health Privacy Board.

2. *Incident Reporting and Response.*

Processes and procedures established by DOST-ICTO for detecting and reporting the occurrence of information security events (by human or automatic means) shall be implemented and observed accordingly.

a. All reported incidents must be identified to immediate response actions to deal with the information security incident.
b. All information security incident report must be updated and collected into the information security event/incident database by information security response team member and must notify the team leader/manager and others as necessary.
c. All information security incidents that have been resolved or closed must be reviewed to:
    i. Conduct further analysis, as required;
    ii. Identify the lessons learned from information security incidents;
    iii. Identify improvements to information security and safeguard the implementation;
    iv. Identify the improvements to the information security response management plan as a whole to determine the effectiveness of the processes, procedures, reporting forms and/or the organizational structure.

3. *Notification in the Case of Breach.*

Notification during instances of breach shall be as follows:

a. Each individual whose protected health information has been, or is reasonably believed by the health care provider or the health facility to have been accessed, acquired or disclosed as a result of breach shall be notified within 60 days upon discovery.
b. Health care providers shall have the burden of proof demonstrating that all notifications were made.
c. Notice shall be provided by the health facility or health care provider to the health privacy board and elevated to the National Privacy Commission when necessary. If the breach affects 500 or more individuals, notification must be provided immediately.

3.1. ***Forms of Notification.***

Notification of privacy breach may be in the form of:

a. Individual notice;
b. Media notice. Media notice shall only be applicable if the unsecured protected health information of more than 500 individuals is reasonably believed to have been accessed, acquired, or disclosed during the breach.

3.2. ***Content of Notification.***

a. A brief description of what happened, including the date of breach and the date of discovery of the breach, if known.
b. A description of the types of unsecured health information that were compromised in the breach (such as full name, philhealth number, date of birth, home address)
c. Situations where individuals are at risk due to the breach and the steps that they should take to protect themselves from potential harm resulting from the breach.
d. A brief description of what the Health Care Provider or Health Facility involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
e. Contact procedures for individuals to ask questions or learn additional information, which shall include a telephone number, e-mail address, website or portal address.
f. Contact information of the National Privacy Commission. Email: privacycommissioner@privacy.gov.ph.
g. Contact information of the National Bureau of Investigation (NBI) Office of Cybercrime, the Philippine National Police Anti-Cybercrime Group (ACG).

3.3. ***Delay of Notification.***

If the health privacy board or the National Privacy Commission determines that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, such notification, notice, or posting may be delayed.

Rule 16
Procedures in the Investigation of Complaints Filed Before the Health Privacy Board

1. *General Principles.*

The Health Privacy Board does not have quasi-judicial powers or the power to impose penalties. Parties who voluntarily submit their complaints or issues for resolution may be assisted in clarifying the issues subject of the complaint, and in reaching an amicable settlement. To ensure compliance with the Resolution of the Board, both parties must submit an undertaking under oath or embodies in an affidavit that the parties agree to be bound by the Resolution of the Board.

The Health Privacy Board does not have subpoena powers or powers of contempt. It relies on the documents and evidence voluntarily submitted by the parties. The investigations conducted by the Board shall be fact-finding and summary in nature, without prejudice, however, to the due process of law, and recourse to the National Privacy Commission or proper courts, when necessary.

The Health Privacy Board may be able to assist the parties in clarifying privacy related complaints in health facilities due to the fact that they have a deeper understanding and better perspective of privacy issues concerning personal and sensitive health information. The Resolution of the Health Privacy Board may also serve as support document of cases filed before the National Privacy Commission, or regular courts.

2. *Procedure for Complaint and Investigation.*

2.1. *Complaint.*

A complaint shall be in writing and under oath or embodied in an affidavit.

2.2. *Who May File.*

The complaint may be filed by any person, firm, partnership, association or corporation, through its duly authorized representative.

2.3. *Contents.*

The complaint must be written in a clear, simple and concise language and shall contain the following:

1. Full names and complete addresses of the complainant and the respondent;
2. A brief narration of the material facts which show a violation of the privacy guidelines or related issuance, or the acts or omissions allegedly committed by the respondent amounting to a privacy concern.
3. If the complainant contains personal and sensitive information involving third parties, which information will be disclosed to the Board, the complainant shall include proof that consent of said parties have been obtained with regard to the use, access and disclosure of said personal or sensitive information for purposes of resolving or adjudicating the complaint, before appropriate bodies.
4. If the Complainant is an institution, the complaint shall be accompanied by the incident report or relevant document showing the results of the investigation conducted within the institution.
5. Certified true copies of documentary evidence, and the affidavit/s of witness/es if any.
6. An undertaking of the complaint, or in case of juridical person by a duly authorized representative, under oath or embodied in an affidavit, to the effect that the complainant agrees to abide by the final resolution of the National Health Privacy Board, without prejudice to other legal remedies.

2.4. ***Number of Copies.***

The complainant, together with the documentary evidence and affidavit/s of witness/es, if any, shall be filed in such number as there are respondents, plus two (2) copies for the file. The affidavit/s required to be submitted shall state facts only of direct personal knowledge to the affiant and shall show the competence of the affiant to testify to the matters stated therein. A violation of the foregoing requirement shall be a ground for expunging the affidavit or portion thereof from the record.

2.5. ***Where to File A Complaint.***

A complaint may be filed at the office of the Health Privacy Board.

2.6. ***Evaluation of Complaint.***

The Board shall evaluate the allegations of the complaint (1) to determine whether it involves a violation of the Privacy Guidelines or issues involving privacy of health information and (2) if based on its allegations, there is reason to believe that there is a violation of the Privacy Guidelines or related issuances. If both conditions are not satisfied, the complaint shall be dismissed.

2.7. ***Issuance of Requests to Appear.***

1. On the basis of the complaint, if there is reason to believe that there is a violation of the Privacy Guidelines, the Board shall request, in writing, the respondent to appear before it, furnishing the said respondent a copy of the complaint, and requiring the submission of a counter-affidavit within ten days from receiving the said request.
2. If the counter-affidavit contains personal and sensitive information involving third parties, which information will be disclosed to the Board, the respondent shall include proof that consent of said parties have been obtained with regard to the use, access and disclosure of said personal or sensitive information for purposes of resolving or adjudicating the complaint, before appropriate bodies.
3. If the respondent appears before the Board, the respondent, or in case of juridical person by a duly authorized representative, shall be asked to sign and undertaking, under oath or embodied in an affidavit, to the effect that the respondent agrees to abide by the final resolution of the National Health Privacy Board, without prejudice to other legal remedies.

2.8. *Procedure if the Respondent Appears.*

1. The Board shall set a date to convene the parties involved in the complaint, sending notices to the parties, and requesting for them to appear before the National Health Data Privacy Board, with their witnesses, if any.
2. The Board shall ensure that before it convenes the parties:
3. Both complainant and respondent have signed and undertaking that they agree to be bound by the Resolution of the Board.
4. Proof that consent have been obtained from third parties when the affidavits or submitted evidence includes their personal and sensitive information, for purposes of resolving or adjudicating the complaint, before appropriate bodies.
5. The Board may ask clarificatory questions when necessary.
6. The Board shall identify the issues for resolution and mediate in order for the parties to reach an amicable settlement. In case the parties reach an amicable settlement, the Board shall issue a resolution on the agreement between parties, which shall be binding in view of their undertaking. Even if the parties have reached an amicable settlement, but the Board finds that the complaint constitutes a violation of law, it shall prepare a report and recommendation, and submit the same to the proper licensing regulatory or accrediting body, or to the National Privacy Commission.
7. In case the parties are unable to reach an amicable settlement, the complaint shall be submitted for resolution. The Board may request the parties to submit a memorandum containing their arguments on the facts and issues for resolution.
8. The Board shall adjudicate on the issues and issue a resolution containing its recommendation. The resolution shall be binding on the parties in view of their undertaking. Its resolution, with supporting documents shall be submitted to the proper

licensing regulatory or accrediting body, or to the National Privacy Commission, for appropriate action, if necessary.

9. The minutes of the proceeding shall be filed and maintained.

2.9. *Procedure if the Respondent does not Appear.*

If the Respondent does not appear before the Board, the Board shall resolve the complaint on the basis of the affidavits and documents submitted by the complainant. Its resolution, with supporting documents shall be submitted to the proper licensing regulatory or accrediting body, or to the National Privacy Commission, for appropriate action, if necessary.

3. *Resolution.*

The Board shall furnish the parties with copies of its resolution.

Rule 17
Penalty Clause

1. Penalties to be imposed shall be in accordance with the Penalty Clause provided in the Joint DOH-DOST-PhilHealth Administrative Order on the Privacy Guidelines for the Implementation of the Philippine Health Information Exchange.

ANNEX 1.0
REFERENCES:

- AO 2016-0002- Privacy Guidelines for the Implementation of the Philippine Health Information Exchange
- Data Protection Act of 1998
- HIPAA Privacy Rule
- Philippine eHealth Strategic Framework and Plan
- Philippine Health Information Exchange Architecture
- R.A. 10173- Data Privacy Act of 2012
- Aguilar, R. (2015). *Social Media and Medical Professionalism: A Manifesto from #HealthXPh*. Retrieved from http://healthxph.net/manifesto

- Australian Commission on Safety and Quality in Health Care, *Framework for Australian clinical quality registries.* Sydney. ACSQHC, March 2014.
- British Medical Association. *Using Social Media: Practice and Ethical Guidance for Doctors and Medical Students.* Retrieved from http://www.bma.org.uk/support-at-work/ethics/medical-students-ethics-tool-kit/students-and-social-media
- Department of Health, NCHFD. (2010). *Hospital Health Information Management Manual 3rd Edition,* Manila, PH : Department of Health.
- C.Evans., D. Laggui., A. Salvador., (2013). *Information Security Incident Response Manual* DOST-ICTO.
- Gliklich, RE. Dreyer, NA. eds. (2007) *Registries for Evaluating Patient Outcomes: A User's Guide*. AHRQ Publication No. 07- EHC001-1. Rockville, MD: Agency for Healthcare Research and Quality.
- Grance, T., Jansen, W. (2011). *Guidelines on Security and Privacy in Public Cloud Computing.* Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
- Grant Thornton (2013). *Third-Party Relationships and Your Confidential Data. Assessing Risk and Management Oversight Processes.* Retrieved from https://www.grantthornton.com/~/media/content-page-files/health-care/pdfs/2013/HC-2013-AIHA-wp-HIPAA-rule-data-control-concerns.ashx
- Health Information Technology for Economic and Clinical Health Act. (2009). Retrieved from https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf
- Herold R., Beaver K. (2015). *The Practical Guide to HIPAA Privacy and Security Compliance. 2nd edition*. Boca Raton, FL: CRC Press.
- Hosek S., Straus S. (2013). *Patient Privacy, Consent and Identity Management in Health Information Exchange. Issues for the Military Health System.* Santa Monica, CA: RAND Corporation.
- National Council of State Boards of Nursing. *A Nurse's Guide to the Use of Social Media.* Retrieved from https://www.ncsbn.org/NCSBN_SocialMedia.pdf
- Newton, J., Garner, S., Disease Registers in England. (Feb 2002). Institute of Health Sciences,
- Office of Civil Rights Headquarters. *Health Information Privacy.* Retrieved from http://www.hhs.gov/hipaa/index.html.
- Patdu, I. (2016). *Recommendations for Social Media Use in Hospitals and Health Care Facilities*. Philippine Journal Of Otolaryngology Head And Neck Surgery, 31(1), 6-9. doi:10.3860/pjohns.v31i1.3548
- PHIC *Human Resources Security document*.
- World Health Organization. *Definition and Typology of Violence.* Retrieved from http://www.who.int/violenceprevention/approach/definition/en/

- Wiles,R., Prosser,J., Bagnoli A., Clark A., Davies K., Holland, S., Renold E., (2008). *Visual Ethics: Ethical Issues in Visual Research*. Retrieved from http://eprints.ncrm.ac.uk/421/1/MethodsReviewPaperNCRM-011.pdf