



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

JOINT ADMINISTRATIVE ORDER

No. 2015-2016-0002

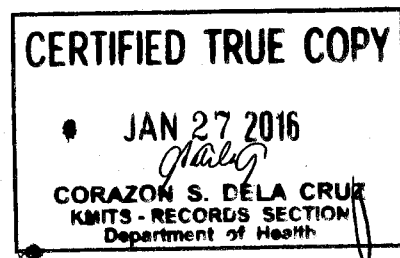
SUBJECT: Privacy Guidelines for the Implementation of the Philippine Health Information Exchange

I. RATIONALE/BACKGROUND

The Constitution mandates the protection and promotion of the right to health of the people and requires the adoption of an integrated and comprehensive approach to health development.¹ The fundamental law likewise recognizes the vital role of communication and information technology in nation-building.² Thus, in the goal of achieving universal healthcare, one of the strategic instruments is to develop the health information system in the country.³ In the 2011-2016 National Objectives for Health, the establishment of a functional eHealth infrastructure at various levels of health care delivery⁴ is expected to revitalize evidence-based policy and program development towards the provision of accessible, quality, affordable, efficient, and safe health for all Filipinos.

As the central agency primarily responsible for the formulation, planning, implementation, and coordination of policies and programs in the field of health,⁶ the Department of Health (DOH), in collaboration with Department of Science and Technology, and the Philippine Health Insurance Corporation, advances the implementation of the Philippine Health Information Exchange (PHIE) to attain the national eHealth vision. The PHIE provides the infrastructure for sharing of health information among participating health care providers (PHCP) involved in the treatment and care of patients. The PHIE harmonizes health data coming from different electronic medical record systems and hospital information systems to provide accurate, relevant, and timely data that shall serve as basis of health policy and health program implementation. The PHIE will also allow the coordination of treatment and care of participating patients through a unified view of health records shared among health care providers.

The implementation of the PHIE involves collection and processing of health information, consisting of both personal and sensitive information. The confidential nature of any information obtained by a physician in the course of treating a patient is a long-established doctrine.⁷ The utilization of information and communication technology to the processing health information only underlines the paramount issue of the right of the patient to medical privacy.



The right to privacy is enshrined in the Constitution.⁸ This right is further articulated in existing legislation, at the forefront of which is the Data Privacy Act of 2012.⁹ These laws,¹⁰ including legislation that specifically provides for health privacy,¹¹ establish the directive for data protection and reinforce the right of the patient to data privacy.

The PHIE serves a public health purpose but its benefits will be fully realized only if its implementation is grounded on respect for privacy rights. This Order provides guidelines for the application of data protection and privacy principles in the implementation of the PHIE.

II. DECLARATION OF PRINCIPLES

This Order complements the following issuances, resolutions or provisions:

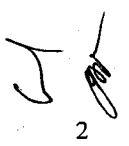
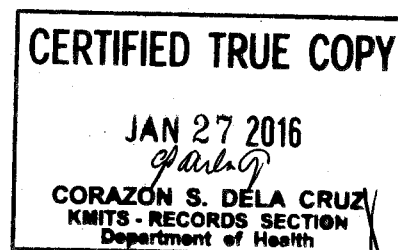
Primacy of human rights. The Constitution declares that the State values the dignity of every person and guarantees full respect for human rights.¹² Health has long been affirmed as a fundamental human right recognized universally.¹³ The right to privacy is also an important human right guaranteed by the Constitution,¹⁴ and further expounded in the Data Privacy Act of 2012.¹⁵

*Vital role of communication and information technology in nation-building.*¹⁶ The order complements the Philippine Digital Strategy 2011-2016 which provides for the national strategy to harness the potential and power of information and communications technology to support the attainment of the government's obligations to the Filipino people, and the Philippines Development Plan 2011-2016 which intends to prepare the country to take advantage of opportunities in a digital economy and knowledge societies.

Improvement of health information systems for public health. The Philippines adopts the generally accepted principles of international law as part of the law of the land.¹⁷ The country is a signatory to a number of global agreements such as the Millennium Development Goals, the Geneva Declaration on the World Summit on Information Society, and the 58th World Health Assembly, wherein the Philippines has pledged to meet specific commitments. These include the adoption of information and communication technology to improve and extend health care and health information systems for public health purpose, and mobilization of multi-sectoral collaboration to develop an overall national eHealth strategy for the implementation of eHealth and health data standards.

Achievement of better health outcomes. This Order supports the 2011-2016 National Objectives for Health¹⁸ and related regulations to utilize ICTs to provide better health services to Geographically Isolated and Disadvantaged Areas, support attainment of Millennium Development Goals, and contribute to the goal of universal healthcare.

Protection of Health Information Privacy. This Order adopts the principles of transparency, legitimate purpose and proportionality contained in the Data Privacy Act of 2012²⁰ for the processing of health information and acknowledges the need to implement security measures for data protection. It adheres to the duty of maintaining confidentiality of patient's medical records and health information as provided by the law, Rules of Court, and the Code of Ethics adopted by the different healthcare providers.



2

III. ETHICAL AND LEGAL STANDARDS

The PHIE upholds universal principles of ethics, legal standards and guiding principles provided by Philippine laws, international instruments, rules and other policies. (See Annex 1.0)

IV. SCOPE OF APPLICATION

1. This Order shall apply to the Philippine Health Information Exchange system, Participating Health Care Providers, and any natural or juridical person involved in the processing of health information within the PHIE framework.
2. This Order shall also apply to patients who have given consent to participate in the PHIE and who have allowed sharing of personal health information among participating health care provider for purpose of treatment and care coordination.

V. OBJECTIVES

This Order implements guidelines for the processing of health information, to ensure that public health goals are achieved and the quality of patient care is improved through utilization of information and communication technology, while protecting the privacy of patients and their health information.

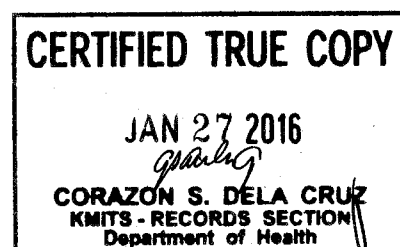
Specifically, this Order shall:

1. Define and limit the circumstances in which an individual's health information is collected, accessed, used, disclosed or otherwise processed.
2. Provide parameters for obtaining consent from the patient for participation in the PHIE.
3. Define the rights of patients participating in the PHIE.
4. Provide guidelines for data protection.

VI. DEFINITION OF TERMS (See Annex 2.0)

VII. GENERAL GUIDELINES

1. The Philippine Health Information Exchange (PHIE) shall be **an integral component of the healthcare delivery system**. It is part of the health services available to all patients. Its implementation shall promote public health and improve total patient care while safeguarding the right to privacy of every individual.
2. The processing of health information within the framework of the PHIE shall be to the extent necessary for the following purposes:
 - a. To have a repository of the country's health information and real time data as basis of health policy, decision-making, and the implementation, monitoring and review of health programs.
 - b. To improve quality and accessibility of health care services, health education, social health insurance, and implementation of other health programs.
 - c. To allow information exchange between participating health care providers for treatment and care coordination purposes.
3. The right to privacy of health information shall be protected. The processing of health information shall be in accordance with law, and shall adhere to the principles of transparency, legitimate purpose and proportionality:



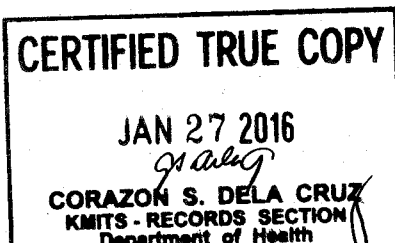
3

- a. Patients shall have a right to adequate information on matters relating to the processing of their health information, including the nature, purpose and intended use of processing.
 - b. Health information shall be processed fairly and lawfully.
 - c. The processing of health information shall not exceed that which is necessary for the purpose of processing, and limited only to data that is relevant or accurate.
4. The PHIE under the Department of Health and the Philippine Health Insurance Corporation (PhilHealth), DOH attached agencies, participating health care providers, and any other natural or juridical person who controls the processing of health information shall have the duty of implementing reasonable and appropriate measures for data protection.
- a. Data protection policies shall be implemented for every stage of the processing of health information.
 - b. Measures for data protection shall include organizational, physical and technical strategies, which shall include policies for evaluation, monitoring and review of operations and security risks.
 - c. The implementation of the Philippine Health Information Exchange shall aspire to develop best practices in all stages of data processing, bearing in mind the state of information and communication technology and generally observed privacy and security standards for data protection.
5. The PHIE shall maintain an online portal or website, which conveys information on the operations of the PHIE and its operators, researchers, partners and consultants, in ways that inspire confidence in its transparency, relevance, governance, operational excellence, privacy protection, and ethical standards. The PHIE online portal shall also be developed to provide health education and to allow patients access to information relating to their health.

VIII. SPECIFIC GUIDELINES

A. Collecting and Processing of Health Information

1. Processing of health information shall be allowed in any of the following cases:
 - a. The processing of personal health information by a healthcare provider is allowed if necessary for purposes of medical care and treatment, provided that the healthcare provider ensures the confidentiality of medical records, pursuant to its ethical and legal duties to patients.
 - b. Processing of health information shall be allowed in cases expressly provided by law, including mandatory reporting requirements. Disclosure of health information shall involve only the minimum necessary information required by law.
 - c. Depending on the use, case, services, and level of sensitivity of the information, data containing complete patient information may be de-identified, anonymized, encrypted, or masked.
 - d. The processing of personal health information shall be allowed if the patient has given his or her consent for participation in the PHIE to allow sharing of personal health information with other PHCP, for purpose of care and treatment coordination, and health care access and quality improvement.
2. De-identification is the removal of identifiers to protect against inappropriate disclosure of personal information. In de-identification of health information, the following identifiers are removed:
 - a. Names;
 - b. Date of birth (except year), provided that ages over 89 shall be aggregated into a single category of "age 90 or older," and other dates (except year) directly related to patient;
 - c. Address other than city or province;
 - d. Telephone or fax numbers;
 - e. Electronic mail addresses;
 - f. Government issued unique identification numbers, such as numbers issued by the Philippine Health Insurance Corporation or Social Security System;
 - g. Medical record, health plan beneficiary and account numbers;
 - h. Certificate or



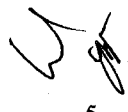
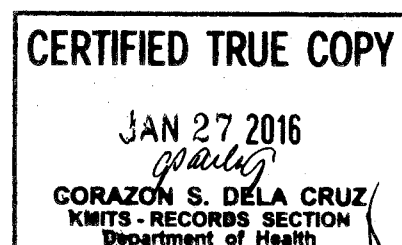
license numbers; i. Vehicle or device identifiers; j. Web universal resource locators or Internet Protocol address; k. Biometric identifiers; l. Full-face or comparable photographs; and, m. Any other unique identifying number, or code.

3. In the processing of health information, the following must be observed:

- a. In all cases, where processing of health information is allowed, the patient shall be informed of the purpose for the collection and further processing of health information, which shall include the purposes for processing information within the PHIE specified in Sec. 2 of this Order. The data collected shall be adequate and not excessive in relation to the declared purpose, and shall not be used other than for the purpose specified at the time of collection.
- b. The PHCP collecting health information shall endeavor to maintain completeness and accuracy of patient's medical record, regardless of the patient's participation in the PHIE.
 - i. Inaccurate or incomplete data must be rectified or supplemented, provided that any amendment made on the medical record shall be documented.
 - ii. If the amendment is made on contents of the medical record, the PHCP shall notify the PHIE, in accordance with the Incident Report and Mitigation Policy provided in Joint Administrative Order No. ____ [Implementation of the PHIE]. Upon reasonable request of the patient, any third party who may have previously received the processed health information shall also be notified.
- c. The entry of data in the medical record of the patient shall be standardized in accordance with the DOH policy on standardization and interoperability.
- d. Health information, in a form that permits identification of patients, shall not be retained longer than necessary for the declared purpose. The retention period shall observe the period recommended by the DOH for retention of paper-based health records.

4. For purposes of processing of Health Information of a patient participating in the PHIE, the following provisions shall apply:

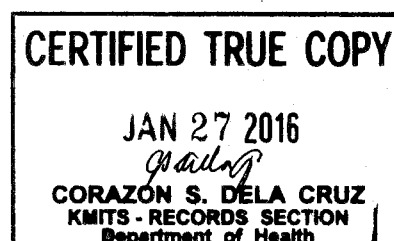
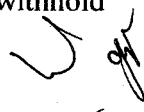
- a. **Creation of a Shared Health Record**
 - i. In order to have a single unified view of the health information of a patient, the PHCP shall prepare a medical record to be shared between health facilities, which shall be referred to as the Shared Health Record (SHR).
 - ii. The Shared Health Record shall follow a prescribed or allowable form. It shall contain pre-determined data fields, consisting of information relevant and necessary for the treatment and care of a patient, but excluding information that must be kept confidential under the law.
 - iii. The Shared Health Record shall contain accurate and relevant information and shall be kept up to date in so far as may be practical.
 - iv. The use of the Shared Health Record for use in the PHIE requires consent from the patient.
- b. **Guidelines for Consent**
 - i. The consent process shall be integrated in PHIE policies and shall aim to alert patients and healthcare professionals on privacy rules and processes for mutual recognition of certain duties, responsibilities, and rights. It shall be complemented by other mechanisms and processes meant to enhance patient autonomy and privacy.
 - ii. The consent of the patient for participation in the PHIE shall be obtained prior to processing of health information. The patient should understand that health information provided to the PHCP for purposes of medical treatment shall be used in the preparation or updating of the Shared Health Record, and that the same information shall be de-identified and transmitted to the PHIE Health Data Warehouse for public health purposes.



5

- iii. In consenting to participate in the PHIE, the patient understands that the Shared Health Record shall be transmitted and further processed in the PHIE for the purposes of coordinating the treatment and care of the patient, improving the quality and accessibility of health care services, and for complying with requirements of other laws for the benefit of the patient.
 - iv. In cases where a patient has previously consented to participate in the PHIE and the patient consults with another participating health care provider, the Shared Health Record shall be made accessible to the other PHCP only if patient consents to its use for purposes provided in the preceding paragraphs. For the purpose of sharing with participating health care providers, only the information contained in the Shared Health Record will be accessible to a PHCP.
 - v. The patient participating in the PHIE shall be informed of the following:
 - (1) Information to be included in the Shared Health Record
 - (2) Existence of security measures for the protection of health information against unauthorized access, accidental or unlawful alteration, disclosure and destruction and any other unlawful processing.
 - (3) Participation in the PHIE requires patient consent, which may be revoked or reinstated at the option of the patient.
 - vi. The PHCP shall also provide the consenting patient with instructions on how to contact the PHCP for concerns related to participation in the PHIE, including the right to request for correction of erroneous entries in the Shared Health Record.
 - vii. Patient shall also be directed to the PHIE website which shall contain information on the nature and purpose of PHIE, intended use of health information, scope and method of PHIE operations, data protection policies being implemented, rights of patients under PHIE, relevant laws and regulation, and any updates or new regulations of public concern.
- c. Rights of Patient participating in PHIE
- i. The patient has a right to be informed that his or her health information is being processed. The patient shall also be informed of the nature and purpose for processing health information, as provided in Sections 2 and Section 8(b)(3) of this Order.
 - ii. The patient shall have a right to be informed about the general operations involved in the processing of health information, and the existence of security measures for data protection.
 - iii. Patient shall have a right to be notified prior to amendment of any information supplied or declared to patient.
 - iv. The patient shall have a right to demand for reasonable access on the contents of processed health information and any further processing, disclosure or amendments made on the Shared Health Record from the time patient consented to participate in the PHIE. A copy of the Shared Health Record may be made available to the patient upon request, subject to administrative fees that the PHCP or PHIE may require.
 - v. The patient shall be advised of the procedure by which he or she can exercise his or her rights, which shall include:
 - (1) Requesting correction of erroneous information coursed through the involved PHCP or by using PHIE online request for amendment provided that retracted information shall still be accessible.
 - (2) Revoking or reinstating consent previously given to participate in PHIE
 - (3) Reporting untoward incidents related to the processing of health information
 - d. Consent of patient, when required by this Order, shall be recorded or documented and may be written or electronic. Rules on the use of biometric or other technical means for obtaining consent may be provided for by the PHIE Governance Structure.
 - e. Refusal by a patient to give consent to participate in the PHIE shall not be a ground to withhold



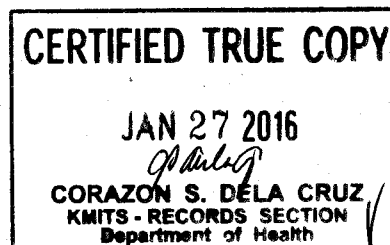
medical treatment or assistance, or any benefits under existing national or social health insurance.

B. Access of Health Information

1. Access to health information by members of the PHIE Governance Structure and participating Health Care Providers shall be in accordance with PHIE issuances.
 - a. The PHIE and the PHCP shall implement a role-based access control where only authorized users are allowed to access the health information, to the extent necessary for their roles.
 - b. The PHIE and the PHCP shall also maintain a user record database to monitor any access and all health information transactions.
2. The PHIE Governance Structure shall authenticate the users with authority to access the processed health information in accordance with PHIE issuances. The PHCP shall be responsible for implementing procedures for authenticating authorized users within their health facility.
3. Access to stored health information shall not be allowed in a location other than within PHIE, Philhealth or the PHCP. All individuals with access to health information shall be bound by contract or legal duty to protect the shared health information.
4. Access to the Shared Health Record shall be allowed in the following cases:
 - a. The patient gives consent to access the Shared Health Record.
 - b. The patient is physically or legally incapable of giving consent, and access to the Shared Health Record is necessary to protect the patient's life or health.
 - c. After the death of a patient, the Shared Health Record may also be accessed to facilitate organ and other tissue donation, if the deceased made pre-arrangements for such access.
 - d. The Shared Health Record may be accessed upon request of the patient, for the patient's own treatment, payment transactions, other health insurance prerequisites, employment records, when required by contract to which a patient is a party, and other reasonable use, to the extent necessary for the purpose.

C. Use and Disclosure of Health Information

1. The use of health information shall be limited to the purposes specified in Sec. 2 of this Order. Only de-identified health information shall be stored in the PHIE Health Data Warehouse. Patient medical records that contain identifiable health information shall be stored in the PHCP as part of the regular operations of the PHCP, provided that if patient consents, the Shared health Record shall be stored and further processed in the PHIE.
2. The Department of Health may order the use and disclosure of personal health information, to the extent permitted by law, but only in case of a serious health and safety threat to the public, which can reasonably be addressed only if the personal health information is used.
3. Any other disclosure of health information to a third party, including requests from a branch, agency or instrumentality of the government, shall not be allowed except if pursuant to the lawful order of the court, or to protect public order and safety as may be prescribed by law, or in cases of emergency to protect life and health of patient when patient is unable to physically or legally give consent to the processing.



4. The confidentiality of privileged information may be invoked in accordance with the provisions of the Rules of Court, and disclosure to any third party of privileged information may be allowed only if with consent of parties to the exchange.

5. The PHCP shall be responsible for limiting the use of the patient's health information stored within the health facility to the purpose specified at the time of collection.

6. The PHCP or PHIE Governance Structure may disclose the Shared Health Record of a particular individual to a third party only upon written request of the patient, or if the patient waives confidentiality of records for purposes complying with contracts to which a patient is a party, such as contracts with health maintenance organizations and health insurance, and employment requirements. The Shared Health Record may also be disclosed in order to comply with a valid court order or pursuant to the express provision of law permitting disclosure without need of patient's consent.

7. The following information may be disclosed for a legitimate purpose:

- a. Aggregate health information
- b. De-identified detailed health information
- c. Health information which must be reported in accordance with mandatory reporting requirements established by law, provided that only the data specified in the law shall be disclosed and that reporting guidelines shall be strictly observed
- d. Health information, to extent necessary to comply with provisions of existing laws and regulations, where consent of patient is not required for disclosure, provided that such laws guarantee the protection of the sensitive, personal and privileged information.

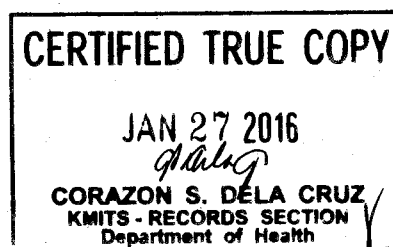
D. Data Security

1. The Department of Health and its attached agencies, the Philippine Health Insurance Corporation, participating health care providers, and any other natural or juridical person who controls the processing of health information shall put in place organizational, physical and technical security measures for data protection.

2. The security measures are intended for the protection of health information and shall aim to maintain the confidentiality, integrity and availability of health data and computer systems, and prevent negligent, unlawful or fraudulent processing, access and other interference, use, disclosure, alteration, loss and destruction of health information.

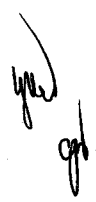
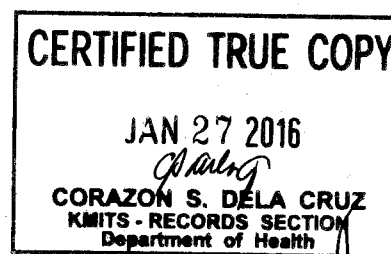
3. Organizational Security Measures:

- a. The PHIE Governance Structure, Philippine Health Insurance Corporation, PHCP or any other natural or juridical person involved in the processing of health information shall designate an individual or individuals who shall be accountable for ensuring compliance with applicable laws and regulations for protection of data privacy. In so far as practicable, there must be a chief privacy officer to manage the privacy aspect in the different areas of the operations, and who shall plan, implement and evaluate policies and programs for data privacy and security.
- b. The processing of health information shall be done by duly authorized or mandated agencies, bodies or individual, subject to PHIE issuances. Contracting with third parties for the sole purpose of processing health information may be allowed subject to approval by the PHIE Governance Structure based on requirements to be determined by authorized representatives of DOH, PhilHealth, and DOST.



8

- c. A security policy shall be implemented, which shall include (but not limited to):
- i. A protocol and design for collection of health information, including procedures for obtaining consent.
 - ii. A process for accreditation and authentication of authorized users to be granted access to the PHIE system
 - iii. Procedures to limit the processing of health information, to ensure that it is only to the extent necessary to the declared and specified purpose at time of collection.
 - iv. Implementing an access management policy to control and monitor individuals with access to shared health information, which shall include role-based access control and maintenance of a secure user record database.
 - v. A protocol to be followed in case of security breach or technical problems, including procedures for investigation, correction and mitigation of any damage that might result due to the security incident.
- d. The PHIE Governance Structure, PHCP or any personal information controller must regularly monitor the system for security breach or any other irregularity that may compromise the privacy or integrity of the shared health information.
- e. The PHIE Governance Structure, PHCP or any personal information controller must implement a procedure for incident reporting. The incident report, in so far as may be applicable, shall contain the following elements:
- i. Date of occurrence or discovery of incident or security breach
 - ii. Nature and description of incident or security breach
 - iii. Manner by which shared health information was compromised
 - iv. Identity of unauthorized parties, if any, who may have accessed the health information
 - v. Measures taken to address or correct breach
 - vi. Any other information that may be relevant
- f. The procedure for incident reporting in the PHIE shall be in accordance with Incident Report and Mitigation Policy provided in Joint Administrative Order No. ____ [Implementation of the PHIE].
- g. Any individual involved in the processing of health information shall maintain the confidentiality of medical records, and any information about a patient that may come to his or her knowledge in the course of performing his duties shall not be disclosed to any third party. The duty of confidentiality shall form part of the terms of engagement or employment of any individual involved in the processing of health information, and shall continue even after the individual leaves the public service, transfers to another position or upon termination of employment or contractual relations.
- h. The PHCP shall promptly notify the PHIE and affected patients when personal health information are reasonably believed to have been acquired by an unauthorized person, and that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. In case the breach occurs within the PHIE, the PHIE shall likewise notify the affected patients, under the same conditions.
- i. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the PHCP to address the breach.
 - ii. Notification to affected patients may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.
- i. Training on privacy and security policies shall be conducted for benefit of individuals involved in the processing of health information.
- j. The privacy and security practices in the PHIE, PHCP or any personal information controller shall be documented, and regularly reviewed and evaluated.



4. Physical Security Measures:

- a. The PHIE Governance Structure, PHCP or any personal information controller shall implement policies and procedures to limit physical access to its facility and work stations, including guidelines which specify proper use of and access to workstations and electronic media.
- b. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing health information, taking into consideration the environment and accessibility to public.
- c. Policies and procedures shall be implemented to monitor activities in the room or workstation. The duties, responsibilities and schedule of individuals involved in the processing of health information shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time.
- d. The PHIE Governance Structure, PHCP or any personal information controller should implement policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of shared health information.
- e. Policies and procedures to prevent mechanical destruction of files and equipment shall be in place. The room and workstation shall in so far as may be practical be secured against natural disasters, power disturbances, external access and other similar threats.

5. Technical Security Measures:

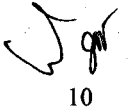
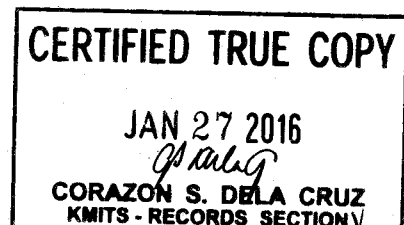
- a. The PHIE Governance Structure, PHCP and personal information controllers shall have in place technical and logical security measures for data protection, including:
 - i. Safeguards to protect its computer network against risks such as accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder functioning or availability of system, and unauthorized access to shared health information that is being transmitted over an electronic network.
 - ii. Hardware, software, and procedural mechanisms to record and examine access and other activity in information systems that contain shared health information, including the monitoring and tracking of any alterations, deletions or additions made to health records.
 - iii. Technical Security measures such as data encryption, authentication process, and other measures to control and limit access to electronic data and health information.
- b. The technical security measures shall be updated and developed with due regard to risks involved in data processing and guided by the requirements of the existing state of technology.

6. The physical and technical security measures prescribed or recommended under relevant laws, rules, and regulations, including appropriate issuances made by DOST-ICTO, shall guide the implementation of security measures.

IX. PENALTY CLAUSE

1. Any participating healthcare provider or patient who shall fail to comply with the provisions of this order or who shall commit any acts that violate the Electronic Commerce Act of 2000, Cybercrime Prevention Act of 2012, and the Data Privacy Act of 2012, in so far as they relate to the operations of the PHIE, shall be penalized with termination of the right to participate in the PHIE, and revocation of all privileges enjoyed pursuant to said participation.

2. Any individual involved in the processing of health information who shall commit any of the acts provided in the preceding section, or who shall fail to observe internal policies or regulations implemented pursuant to the provisions of this Order shall have his or her authorization to access the



10

PHIE revoked, in addition to disciplinary actions imposable under rules of the concerned agency, institution, company or organization.

3. The penalties imposed for violation of this Order shall not be a bar to the criminal prosecution for violation of the Electronic Commerce Act of 2000 (R.A. No. 8792), Cybercrime Prevention Act of 2012 (R.A. No. 10175), Data Privacy Act of 2012 (R.A. No. 10173), the Revised Penal Code or other special laws, whenever applicable. The penalties imposed shall also be without prejudice to any civil or administrative liability under existing laws, rules and regulations for the same acts.

4. The procedure for termination or revocation of rights or privileges shall be in accordance with the Incident Response and Mitigation Policy provided in Joint DOH-DOST-PhilHealth Administrative Order on the Implementation of the Philippine Health Information Exchange.

X. OPERATIONAL BUDGET

The budget required to implement this Joint Administrative Order shall be collectively sourced out from the Offices of the Secretary of Health, Secretary of Science and Technology, and President/CEO of PhilHealth, or any available funds under DOH, DOST and/or PhilHealth, and shall be managed by the Knowledge Management and Information Technology Service of the DOH.

XI. REPEALING CLAUSE

All Orders, Memoranda, Circulars, or other issuances that are inconsistent or contrary to the provisions of this Order are hereby repealed or modified accordingly.

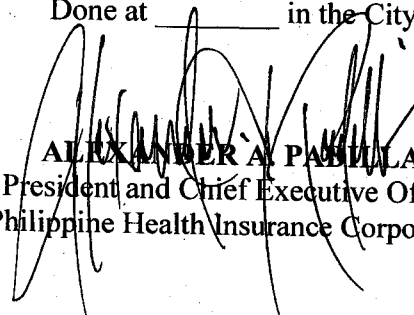
XII. SEPARABILITY CLAUSE

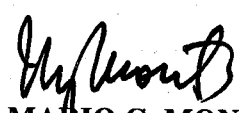
In the event that any provision or part of this Order is declared unauthorized or rendered invalid, those provisions not affected by such declaration shall remain valid and in force.

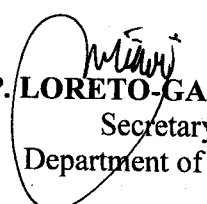
XIII. PUBLICATION AND EFFECTIVITY

This Joint Order shall take effect upon approval/signing by the Secretary of Health, Secretary of Science and Technology, and President/Chief Executive Officer of Philippine Health Insurance Corporation, and fifteen (15) days after its publication in two (2) newspapers of general circulation.

Done at _____ in the City of Manila on JAN 20 2016


ALEXANDER A. PAMBILA
President and Chief Executive Officer
Philippine Health Insurance Corporation


MARIO G. MONTEJO
Secretary
Department of Science and Technology


JANETTE P. LORETO-GARIN, MD, MBA-H
Secretary
Department of Health

CERTIFIED TRUE COPY

JAN 27 2016


CORAZON S. DELA CRUZ
KMITS - RECORDS SECTION
Department of Health

- ¹ PHIL. CONST. art.II §15, art.XIII §11. See also RA 7875, Sec 2.
- ² PHIL. CONST. art.II §24, art. IVX §10
- ³ Aquino Health Agenda (AHA), Administrative Order No. 2010-0036 (2010).
- ⁴ 2011-2016 *National Objectives for Health, Health Sector Reform Agenda Monographs* 114-115 [Manila, Republic of the Philippines - DEPARTMENT OF HEALTH, 2011 (DOH HSRA Monograph No. 12).]
- ⁶ Instituting the "Administrative Code of 1987" [Administrative Code], Executive Order No. 22, Title IX, Chapter 1 §2 (1987).
- ⁷ Hippocratic Oath, available at <http://medical-dictionary.thefreedictionary.com/Hippocratic+Oath> (last accessed Sept. 27, 2014); See also The World Medical Association Declaration of Geneva, Physician's Oath (1948); Code of Ethics, Professional Regulation Commission Board of Medicine, art II §6; See also Code of Ethics, Philippine Medical Association, art 2 §6; Revised Rules of Evidence, Rules of Court, Rule 28 §24(c) (1989).
- ⁸ PHIL CONST. art.III §§1,2,3, 6, 8, 17.
- ⁹ Act Protecting Individual Personal Information in Information Systems in the Government and the Private Sector, Creating for this Purpose A National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], R.A. 10173 (2012).
- ¹⁰ An Act Providing for the recognition and use of electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful use therefor and other purposes, [Electronic Commerce Act of 2000], R.A. 8792 (2000); An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for Other Purpose [Anti-wiretapping law], R.A. No. 4200 §§ 1-2(1965); An Act to Ordain and Institute the Civil Code of the Philippines [NEW CIVIL CODE], Republic Act No. 386, art. 26 and 32 (1950).
- ¹¹ Prevention and Control of HIV/AIDS in the Philippines, Instituting a Nationwide HIV/AIDS Information and Educational Program, Establishing a Comprehensive HIV/AIDS Monitoring System, Strengthening the Philippine National Aids Council, and for Other Purposes, "Philippine AIDS Prevention and Control Act of 1998", Republic Act No. 8504, (February 13, 1998); An Act Instituting the Comprehensive Dangerous Drugs Act of 2002, Repealing Republic Act No. 6425, Otherwise Known as the Dangerous Drugs Act of 1972, as Amended, Providing Funds Therefor, and for Other Purposes, "Comprehensive Dangerous Drugs Act of 2002", Republic Act No. 9165, (June 7, 2002); An Act Defining Violence Against Women and Their Children, Providing for Protective Measures for Victims, Prescribing Penalties Therefore, and for Other Purposes, "Anti-Violence Against Women and Their Children Act of 2004", Republic Act No. 9262, (March 8, 2004); The Child and Youth Welfare Code, Presidential Decree No. 603, Title VIII Chapter 1 art. 166 (1974).
- ¹² PHIL. CONST. art.II §2.
- ¹³ Declaration of Alma-Ata, International Conference on Primary Health Care, Alma-Ata, USSR, 6-12 September 1978, available at http://www.who.int/hpr/NPH/docs/declaration_almaata.pdf (last accessed June 8, 2008).
- ¹⁴ PHIL CONST. art.III §§1,2,6, 8, 17.
- ¹⁵ Act Protecting Individual Personal Information in Information Systems in the Government and the Private Sector, Creating for this Purpose A National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], R.A. 10173 (2012).
- ¹⁶ PHIL. CONST. art.II §24, art. IVX §10
- ¹⁷ Act Protecting Individual Personal Information in Information Systems in the Government and the Private Sector, Creating for this Purpose A National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], R.A. 10173 (2012).
- ¹⁸ 2011-2016 *National Objectives for Health, Health Sector Reform Agenda Monographs* 114-115 [Manila, Republic of the Philippines - DEPARTMENT OF HEALTH, 2011 (DOH HSRA Monograph No. 12).]
- ²⁰ Act Protecting Individual Personal Information in Information Systems in the Government and the Private Sector, Creating for this Purpose A National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], R.A. 10173 (2012).

Annex 1.0. Ethical and Legal Standards

The PHIE upholds universal principles of ethics, legal standards and guiding principles provided by Philippine laws, international instruments, rules and other policies, which include, but are not limited to, the following:

1. The Philippine Constitution, Article III Bill of Rights, Sections 2-3
2. Civil Code of the Philippines Arts. 26 and 32
3. Data Privacy Act of 2012 (Republic Act No. 10173)
4. Cybercrime Prevention Act of 2012 (R.A. No. 10175)
5. Electronic Commerce Act of 2000 (Republic Act No. 8792)
6. The Philippine AIDS Prevention and Control Act of 1998 (Republic Act No. 8504)
7. The Medical Act of 1959 (Republic Act No. 2382)
8. Rules of the Court, Rule 130, Sec. 24
9. Code of Ethics adopted by healthcare providers and health professionals such as the Professional Regulation Commission (PRC) Board of Medicine Code of Ethics and Philippine Medical Association Code of Ethics
10. PHREB National Ethical Guidelines for Health Research 2011 Asia-Pacific Economic Cooperation Privacy Framework 2005
11. WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects 2013
12. WMA International Code of Medical Ethics 2006
13. WMA Guiding Principles for the Use of Telehealth for the Provision of Health Care 2009
14. WMA Statement on the Ethics of Telemedicine 2007
15. eHealth Ethics Initiative 2000
16. WHO Executive Board 115th Session on eHealth 2004 and the 58th World Health Assembly Report on eHealth 2005



Annex 2.0. Definition of Terms

For the purpose of this Order, the following terms are defined:

1	Access	Refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network.
2	Alteration	Refers to the modification or change, in form or substance, of an existing computer data or program.
3	Authentication	The process of verifying that an individual, entity or software program accessing the PHIE is the authorized user the person, entity or program claims to be.
4	Authorization	The process of determining whether a user has the right to access the PHIE and establishing the privileges associated with such access.
5	Confidentiality	A duty to maintain privacy of information and its protection against unauthorized disclosure.
6	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.
7	De-identification	Removal of identifiers to protect against inappropriate disclosure of personal information
8	Electronic medical record	A medical or health record which is which is received, recorded, transmitted, stored, processed, retrieved or produced electronically through computers or other electronic device.
9	Health care provider	A health care institution devoted primarily to 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.
10	Health Data Warehouse	A repository of the country's de-identified health information within the framework of the Philippine Health Information Exchange.
11	Health information	Refers to personal and sensitive information that relates to an individual's past, present or future physical or mental health or condition, including demographic data, diagnosis and management, medication history, health financing record, cost of services and any other information related to the individual's total well-being. For purpose of this Order, health information refer to personal health information which is individually identifiable health information or de-identified health information.
12	Individually Identifiable	Refers to information that contains data that can directly identify the individual or could reasonably be used to identify an individual.
13	Interception	Refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of 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.



14	Issuances	Refer to official write-up or documentation of statements, notices, announcements, and communications.
15	Medical Privacy or Health Privacy	Right to the protection of the confidential nature of personal health information, which includes communications between health care provider and patient, and personal data and information about a patient's condition as contained in medical records.
16	Medical Record or Health Record	Primary repository of information concerning patient health care; a compilation of pertinent facts of a patient's life history including past and present illnesses and treatments entered by health professionals contributing to that patient's care.
17	Participating Health Care Provider (PHCP)	Health Care Providers whose application to participate in the PHIE is approved in accordance with Joint DOH-DOST-PhilHealth AO ____ [Implementation of the PHIE], and through any other procedure promulgated by the DOH for participation.
18	Patient	A person availing of medical consultation, diagnostic examinations, treatment or health care services from a health care provider.
19	Personal information	Refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
20	Personal information controller	<p>Refers to 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.</p> <p>The term excludes:</p> <ul style="list-style-type: none"> 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
21	Principle of Legitimate purpose	Principle that refers to processing of information in accordance with a declared and specified purpose, which must not be contrary to law, morals or public policy.
22	Principle of Proportionality	Principle that refers to processing of information that is adequate, relevant and not excessive in relation to a declared and specified purpose.
23	Principle of Transparency	Principle that refers to processing of information conducted in a manner where an individual is given adequate and relevant knowledge about the nature, purpose, extent and intended use of processing of information, and provided with the right to consent, limit or object to the processing.
24	Privacy	The right of a person to be free from intrusion or disturbance in one's personal and intimate life or affairs. It includes informational privacy, which refers to the right of an individual not to have his or her private information disclosed, including the ability to control what information is disclosed, with whom, and

		for what purpose.
25	Processing	Refers to 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.
26	Public Health	Refers to all organized measures to prevent disease, promote health, and prolong life among the population as a whole. Its activities aim to provide conditions in which people can be healthy and focus on entire populations, not on individual patients or diseases.
27	Security	Refers to the organizational, technical and physical measures to ensure the safety and protection of the health information.
28	Sensitive Personal Information	Refers to personal information: <ul style="list-style-type: none"> 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.
29	Sharing	The process that allows the PCHP to access the patient's health information from the system.