Republic of the Philippines
Department of Health
OFFICE OF THE SECRETARY

JUL 0 9 2020

ADMINISTRATIVE ORDER
No. ~~2019~~ 2020-0030

SUBJECT: **Data Privacy Guidelines on the Processing of Health Information**

I. BACKGROUND AND RATIONALE

The Department of Health (DOH), being the lead government agency in health, is mandated to develop national plans, technical standards, and guidelines on health. In order to uphold the right to health of the Filipino people, the Department collects, analyzes, interprets and disseminates statistical and other relevant information on the country's health situation; require the reporting of such information from appropriate sources; undertake health and medical research; and conduct trainings in support of its priorities, programs and activities.

With the aim of attaining the goals outlined in the Philippine Development Plan 2017-2022, Ambisyon Natin 2040, and the Sustainable Development Goals, and building on the concept of F0URmula One for Health 2005-2010, the medium-term strategic framework for 2017—2022 expands the four pillars of health reforms. They also highlight greater focus on the performance accountability towards the Filipino people, thus, FOURmula OnePlus for Health or F1+, with its tagline "Boosting Universal Health Care". Specifically, on sub-pillar number 4 on Governance, this aims to strengthen leadership and management capacities, coordination, and support mechanisms necessary to ensure functional, people-centered and participatory health systems.

And the National Objectives for Health that should ensure generation and use of evidence in health policy development, decision making, and program planning and implementation.

The processing of health information consists of both personal and sensitive personal information, which only underscores the right of an individual to health privacy. This right is articulated in Republic Act No. 10173 otherwise known as the *Data Privacy Act of 2012* (DPA), which protects the privacy of health information, establishes the directive for data protection, and reinforces the right of an individual to privacy. As the leader in health, the DOH is permitted to the lawful processing of personal data as stated in Sections 4(e), 12 and 13 of the DPA in order to fulfill its mandate.

In compliance with the DPA, this Administrative Order is issued to serve as guidelines for the processing of health information, while ensuring utmost protection of the right to privacy of an individual and their health information.

II. OBJECTIVE

This Order provides guidelines for the collection, use, sharing, and processing of personal and sensitive personal information by DOH, its offices, bureaus, services, units and attached agencies, health facilities and healthcare providers regulated by DOH, to ensure privacy and data security in data processing systems.

III. SCOPE

The guidelines shall apply to all DOH offices, bureaus, services, units and attached agencies; and to both government and private national and local health facilities, healthcare providers, and stakeholders that are involved in the processing of health information.

IV. DEFINITION OF TERMS

The following terms are defined for the purpose of this Order:

1. **Compliance Officer for Privacy (COP)** is an individual or individuals who perform some of the functions of a DPO. *(National Privacy Commission Advisory No. 2017-01)*

2. **Data Protection Officer (DPO)** is an individual who is accountable for ensuring compliance with applicable laws and regulations relating to data privacy and security. *(DPA)*

3. **Data Sharing** is the disclosure or transfer to another government agency of personal data and/or information under the control or custody of a Personal Information Controller (PIC); *Provided*, that a PIC may be allowed to make such disclosure or transfer if it is upon the instructions of the PIC concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor. *(Implementing Rules and Regulations of the DPA)*

4. **Data Subject** refers to an individual whose personal information is processed. *(DPA)*

5. **Health care provider** refers to 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, nutritionist, pharmacist, medical technologist, or other health care practitioner. *(DOH, Department of Science and Technology (DOST) and Philippine Health Insurance Corporation (PHIC) Joint Administrative Order (JAO) No. 2016-0002)*

6. **Health facility** refers to institutions, whether stationary or mobile, land based or otherwise, that provides healthcare and other healthcare-related establishment which provides diagnostics, therapeutic, rehabilitative, palliative and/or related health care services. *(DOH AO No. 2018-0016)*

7. **Health information** refers to the 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. *(DOH, DOST and PHIC JAO No. 2016-0002)*

8. **Meaningful use** as the use of certified electronic health record technology to improve quality, safety, efficiency, and reduce health disparities, engage patients and families in their health care improve care coordination, improve population and public health, all the while maintaining privacy and security. *(Centers for Disease Control and Prevention)*

9. **Non-disclosure Agreement (NDA)** a contract by which one or more parties agree not to disclose confidential information that they have shared with each other as a necessary part of doing business together.

10. **Personal information controller or "PIC"** refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes: a person or organization who performs such functions as instructed by another person or organization; or an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs. There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing. *(DPA)*

11. **Personal information processor or "PIP"** refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject. *(DPA)*

12. **Personal data** refers to all types of personal information such as follows:

    a) **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. *(DPA)*

    b) **Sensitive personal information** refers to personal information:
        i. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
        ii. 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;
        iii. 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; and
        iv. Specifically established by an executive order or an act of Congress to be kept classified. *(DPA)*

13. **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. *(DPA)*

14. **Secure Area** refers to an organization's premises protected from unauthorized physical access, damage and interference. *(International Organization for Standardization)*

15. **Stakeholders** generally refers to those agencies and institutions which the Department interacts with in policy formulation, planning, budgeting, implementation, monitoring and evaluation of health sector reform programs, activities, and projects. This includes program beneficiaries, Civil Society Organizations (CSOs), academic institutions, private sector and industry specific groups, and development partners whose interests are in line with pursuing a more harmonized and convergent approach for the effective implementation of the Department's health sector reform agenda. *(DOH Department Order No. 2016-0010)*

V. GENERAL GUIDELINES

a) The DOH, being a repository of health information collected pursuant to its mandate, shall implement the appropriate organizational, physical and technical security measures to maintain the confidentiality, integrity and availability of personal and sensitive personal information in its data processing systems. It shall adhere to data privacy principles of transparency, legitimate purpose and proportionality in the collection, use, sharing, storing and disposal of personal and sensitive personal information.

b) Health Information submitted and shared by health facilities, health care providers and stakeholders shall submit or share health information including personal data required by the DOH, its offices, bureaus, services, units and attached agencies in conjunction with its respective functions, and in accordance with the DPA, its IRR and other relevant laws, rules and regulations. Health information that are submitted or shared shall be for the following purposes:

1. Planning of quality services;
2. Reporting of selected non-communicable diseases, communicable, infectious and other notifiable diseases, including those that pose a serious health and security threat to the public such as, but not limited to:
   - 1.1 Meningitis
   - 1.2 Food Poisoning (Mass);
   - 1.3 Breakthrough epidemic of contagious disease;
   - 1.4 Biological or chemical warfare;
   - 1.5 Emerging and re-emerging communicable diseases;
3. Continuing care to patients;
4. Reporting of physical injury to the Online National Electronic Injury Surveillance System (ONEISS);
5. Reporting of interpersonal violence to proper authorities;
6. Reporting of diseases as registered in the Philippine Integrated Diseases Surveillance and Response;

7. 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.).

c) DOH offices, bureaus, services, units and attached agencies shall comply with the organizational, physical and technical security measures for data protection required by the DPA.

d) Sharing of Personal Data with other government agencies shall only be allowed with the consent from data subjects or when shared pursuant to the constitutional or statutory mandate of the concerned government agency, in which case, the sharing shall be covered by a Data Sharing Agreement (DSA).

e) This Order serves as the terms and conditions of a DSA between DOH and/or its attached agencies, and the government or private national and local health facilities, healthcare providers and other stakeholders involved in the processing of Personal Data and Health Information, as prescribed under the DPA and NPC Circular No. 16-02 dated 10 October 2016.

f) In case of data breach, violation of the rights of the data subject, or any violation of the DPA, it shall proceed in accordance thereto and its IRR.

VI. SPECIFIC GUIDELINES

a. Preprocessing

1. The DOH shall implement a privacy management program, which includes procedures for review and improvement. DOH shall likewise ensure that there is a designated data protection officer or compliance officers for the Department, its offices, bureaus, services, Centers for Health Development (CHD), DOH Medical Centers, Hospitals, Sanitaria, Treatment and Rehabilitation Centers (TRCs) and attached agencies. Whenever appropriate, the Department shall conduct privacy impact assessments on its data processing systems.

2. Consent from the data subject shall be required prior to the processing of health information in all health facilities following the guidelines in the Joint Administrative Order No. 2016-0002 entitled *"Privacy Guidelines for the Implementation of the Philippine Health Information Exchange"*. A consent form from Health Facilities Development Bureau guidelines on Hospital Health Information Management Manual for this purpose shall be incorporated in the admission/confinement forms of hospitals, treatment/health facilities which shall be accomplished prior to the patient's admission or management.

3. A non-disclosure agreement (NDA) shall be executed by DOH consultants/staff who are under the contract of service agreement, and who have access to health information and/or involved in the processing of Personal Data/Health Information, providing penalties thereon in case of breach.

4. In order to afford full respect for the rights of data subjects, the DOH shall make privacy notices, including the contact details of its data protection officer readily accessible in its offices, website and similar areas so that data subjects shall have means of obtaining information and exercise their rights as data subjects.

5. The DOH shall maintain and implement a breach management program. This includes the maintenance of a security policy, accountability tracking system, breach response team and compliance with reporting requirements of the NPC.

b. **Processing**

1. The rights of the data subjects shall be respected and protected at all times in processing data.

2. Any established Information Technology (IT) system for data management shall use applicable encryption methods to ensure security of data at rest, in transit and/or in use.

3. Printed data and records shall be stored in a secure area. Records and archives management shall be in accordance to the National Archives of the Philippines Act of 2007, its IRR and relevant rules and regulations.

4. Data stored in portable data storage device (e.g. DVD, flash drives, external hard drives, tape drives, etc.) shall be encrypted and stored in a secure area.

5. Access to health information shall follow the Health Privacy Code. Such access is specified for the following groups:

    a. Access of Health Care Providers. Only a health care provider directly attending to the patients and authorized entities shall have access to the patient's health information provided that there is an accomplished consent form from the patient.

    b. Access of Patient or Client. Consenting patients or clients shall have the rights to access information on how their Personal Data/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.

    c. Access of Third Party. A third party shall have no access to a patient's Personal Data/Health Information unless the access/disclosure is required by law, or upon a lawful order by a court. A third party accessing Personal Data/Health Information of a patient/individual pursuant to a valid contract where the health care provider/health facility is not a privy, shall not be allowed access to such information without a legal instrument (SPA) executed for such purpose.

6. In processing Personal Data/Health information for research, research institution/individual (public or private) shall comply with the legal and ethical standards in accordance with the National Ethics Guidelines for Health and Health Related Research of 2017 and other pertinent laws, rules and regulations.

7. The DOH shall adopt and implement strategies for the meaningful use of information generated in order to contribute to the implementation of the national health plan, present proposals to appropriate authorities on national issues which have health implications, promote health and wellness, and improve health care delivery system.

8. The DOH in the exercise of its regulatory function over health services and facilities mandates full cooperation and compliance from health care providers in the reporting requirements provided in this Order and other applicable rules and regulations issued by the Department.

VII. ROLES AND RESPONSIBILITIES

a. **Department of Health**

1. **Bureau of Local Health Systems and Development (BLHSD),** as the lead agency in Local Health Systems Development, shall ensure the dissemination and implementation of this Order in the Local Government Units (LGUs) through the CHDs.

2. **Bureau of Quarantine (BOQ),** as the sole public health authority that provides optimum security against the introduction and spread of infectious disease that may pose public health emergency of international concern at all ports of entry, shall institute appropriate and reasonable standards of privacy, confidentiality and security in processing Personal Data/Health Information collected in its performance of the following functions/services:
   a. Vessel and Aircraft Crew or Passengers under surveillance;
   b. Provision of Medical Services (Physical Examination, Vaccinology and Laboratory);
   c. Enforcement of Health and Sanitation among Food Establishments and Food Handlers within the Bureau's area of responsibility; and
   d. Issuance of Quarantine Permits (Human Remains and Biological Specimen).

3. **Centers for Health Development (CHD)**
   a. oversee and implement in their respective regions, compliance with appropriate and reasonable standards of privacy, confidentiality and security on the processing of Personal Data;
   b. capacitate CHD staff including the Human Resources for Health (HRH) on lawful data processing in accordance with the DPA; and
   c. coordinate with LGUs, other local sectors, and stakeholders on the adoption and implementation of this Order.

4. **Dangerous Drugs Abuse Prevention and Treatment Program (DDAPTP)** shall institute appropriate and reasonable standards of privacy, confidentiality and security in the processing and controlling of personal data being compiled/collected in its operations of anti-drug related programs from rehabilitation, aftercare, to follow-up, in collaboration with other agencies.

5. **Disease Prevention and Control Bureau (DPCB)** as the technical authority in disease prevention and control shall:
   a. ensure the appropriate and reasonable standards of privacy, confidentiality and security in the processing and controlling of Personal Data/Health Information;
   b. integrate privacy, confidentiality and security standards in its formulation of national policies and standards for health.

6. **Epidemiology Bureau (EB)** as the technical authority in disease surveillance shall:
   a. develop disease and event surveillance and information system which has sufficient safeguard to privacy, instituting confidentiality and security standards and measures in the performance of its mandate such as, but not limited to, outbreak investigation, disease surveillance, epidemiologic surveys, disease registries and contact tracing; and
   b. safeguard the privacy and confidentiality of Personal Data/Health Information as the designated custodian and safe keeper of epidemiological data, capacities and capabilities of the Department.

7. **Field Implementation and Coordination Team (FICT)**
   a. oversee and coordinate with CHD, DOH retained hospitals, special hospitals, sanitaria, and Drug Abuse Treatment and Rehabilitation Centers(DATRCs) the compliance to the standards of privacy, confidentiality and security on the processing and controlling of personal data; and
   b. formulate recommendations and internal policies which can be followed by the CHDs, DOH retained hospitals, special hospitals, sanitaria, and DATRCs in relation to the compliance with this Order, the DPA and its IRR, and other relevant rules and regulations.

8. **Health Emergency and Management Bureau (HEMB)** shall comply with the appropriate and reasonable standards of privacy, confidentiality and security in processing of Personal Data/Health Information necessary in the discharge of its functions, as stated below:
   a. act as the lead agency in health emergency response services, including referral and networking systems for trauma, injuries and catastrophic events;
   b. innovation/formulation of new strategies for responding to emerging health needs; and
   c. act as lead agency in health emergency, prevention and mitigation, preparedness and response, recovery and rehabilitation.

9. **Health Facilities and Services Regulatory Bureau (HFSRB)** shall protect and ensure the confidentiality of documents submitted to the Bureau such as but not limited to, documents for compliance, complaints and its documentary evidence, and Annual Statistical Reports, by adopting the following policies:
   a. total access to all records shall be limited to administrators, evaluators, and validators of HFSRB including CHD-RLEDs;
   b. limited access to such records shall be given to other DOH Bureaus; and
   c. only de-identified data, and aggregated values/data shall be given to external stakeholders such as but not limited to researchers, students, etc.

10. **Health Facilities Development Bureau (HFDB)**
    a. develop guidelines and standard procedures for ensuring privacy, confidentiality and security of health information in relation to the development, planning, operations, management and maintenance of health facilities, their programs and services; and
    b. provide access to health information collected and mandatory submission of these information to DOH and PhilHealth, as indicated in the UHC Law
    c. coordinate with the national and sub-national reference laboratories and other health laboratories through the National Health Laboratory Network to ensure that privacy, confidentiality and security of health information in their processes are compliant with this Order.

11. **Health Human Resource Development Bureau (HHRDB)**
    a. coordinate learning and development opportunities to be available to Human Resource for Health in relation to the implementation of this Order; and
    b. finance the issuance and creation of the program, hiring of additional personnel and training of the designated Data Protection Officer.

12. **Health Promotion and Communication Services (HPCS)**
    a. institute privacy, confidentiality and security standards in its public information campaign on health and well-being, and in its provision of timely and relevant information on health risks and hazards to the public;
    b. ensure confidentiality and proper handling of captured Personal Data/Health Information in its health advocacy and health promotion activities, particularly in its use of different communication platforms;
    c. develop a communication plan on the privacy of health information for the public, including the guidelines set forth in this Order; and
    d. advocate, through information education campaign, the guidelines set forth in this order.

13. **Knowledge Management Information Technology Service (KMITS)**
    a. lead to formulate plans, policies, programs, and standards for systems and processes improvement, including systems and software development, that will ensure the privacy, confidentiality and security of data pursuant to the DPA;
    b. develop and manage the DOH ICT Infrastructure and provide ICT related – services that will strengthen the security of data;
    c. responsible for the management/maintenance of the repository of DOH health data;
    d. see to it that All DOH offices shall have a designated Data Protection officer (DPO) & to have capacity and capability building with coordination with National Privacy Commission (NPC); and
    e. develop process which shall be included in the Manual of Procedure (MOP) for this issuance.

14. **National Nutrition Council (NNC)**
    a. ensure compliance to the standards for privacy, confidentiality and security under the DPA in relation to nutrition data harmonization, data basing, and to its design and implementation of quad media nutrition promotion, monitoring and evaluation systems, on nutrition situation and capacities;

b. orient barangay nutrition scholars on the guidelines set forth in this Order; and
c. support the HPCS through the agency's media network.

15. **National Voluntary Blood Services Program (NVBSP)** shall institute appropriate and adequate privacy, confidentiality and security standards for the health information systems of its programs in voluntary blood donations, and in its provision of adequate supply of safe blood, in accordance with the DPA, its IRR and this Order.

16. Philippine National AIDS Council shall institute appropriate and adequate privacy, confidentiality and security standards for the health information systems of its programs in HIV/AIDS, in accordance with the DPA, its IRR and this Order.

b. **Health Care Providers/Health Facilities, and other Private Entities** shall:
   a. ensure confidentiality, integrity and availability of patient health information;
   b. ensure that records are stored, retained and disposed of in accordance to the guidelines set by the DOH Hospital Management Manual and National Archives of the Philippines (NAP);
   c. comply with the minimum data sets, data generation, collection and aggregation methods and designate qualified staff as required by the DOH;
   d. collect and use, in a timely and efficient manner, relevant, accurate, quantitative and qualitative data, for the delivery of its patient care services;
   e. make its clinical/medical records readily available and accessible, in order to facilitate patient care, and submission to the Department's authorized representative. Its clinical/medical records shall be kept confidential, securely stored, and maintained in accordance with the DPA, and other relevant statutory requirements and codes of practice;
   f. provide access on all Personal Data/Health Information it collected/compiled, to concerned DOH offices, bureaus, services and units through their respective authorized representatives, in conjunction with their respective functions;
   g. In case of outbreak investigations, disease surveillance, contact tracing and other similar actions, performed by the Department pursuant to its mandate, when immediate access to Personal Data/Health Information is necessary to protect public health, or in case of emergencies and calamities, health care providers, health facilities and other private entities shall provide unimpeded access to Personal Data/Health Information in their possession and shall ensure that proper internal procedure is in place to facilitate prompt action.

VIII. NON-COMPLIANCE

Failure to comply with this Order shall be punished administratively, civilly and criminally as permitted by applicable laws and in accordance with the penalties set forth in Republic Act No. 10173, also known as the Data Privacy Act of 2012 and its Implementing Rules and Regulations.

IX. REPEALING CLAUSE

Provisions from previous and/or related issuances inconsistent or contrary with the provisions of this Order are hereby revised, modified, and rescinded accordingly. All other provisions of existing issuances which are not affected by this Order shall remain valid and in effect.

X. EFFECTIVITY

This Administrative Order shall take effect immediately.

FRANCISCO T. DUQUE III, MD, MSc
Secretary of Health

CERTIFIED TRUE COPY
JUL 15 2020
CORAZON S. DELA CRUZ
KMITS - RECORDS SECTION
Department of Health