



Republic of the Philippines
DEPARTMENT OF HEALTH
NATIONAL PRIVACY COMMISSION

April 24, 2020

JOINT MEMORANDUM CIRCULAR

No. 2020- 0002

SUBJECT: Privacy Guidelines on the Processing and Disclosure of COVID-19 Related Data for Disease Surveillance and Response

I. BACKGROUND

In pursuit of disease surveillance and response against the coronavirus disease 2019 (COVID-19) in the country, and pursuant to Republic Act (RA) 11332 (Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act), the Department of Health (DOH), being the principal health agency in the country, collects, processes and disseminates COVID-19-related data; requires the reporting of such data from appropriate sources; and undertakes apropos epidemiologic investigations and biomedical researches.

The collection and processing of COVID-19-related data consists of both personal and sensitive personal information. The confidential nature of these data only underscores the primacy of right of the patient to health privacy. This right is articulated in RA 10173 (Data Privacy Act of 2012 [DPA]), which specifically provides for health privacy, establishes the directive for data protection, and reinforces the right of the patient to data privacy.

In response to the growing privacy concerns raised by various stakeholders during this current COVID-19 health situation, and in upholding RA 11332 and RA 10173, the Department of Health and the National Privacy Commission (NPC) hereby issue these guidelines on the application of data protection and privacy principles in the collection, processing and disclosure of COVID-19-related data in pursuit of disease surveillance and response.

II. OBJECTIVE

This Joint Memorandum Circular implements the guidelines for the collection, processing and disclosure of COVID-19-related data in pursuit of disease surveillance and response, while protecting the data privacy rights of patients and individuals and ensuring the confidentiality, integrity, and availability of their personal data.

III. SCOPE AND COVERAGE

This Joint Memorandum Circular shall apply to the implementation of the COVID-19 disease surveillance and response; and shall cover all public and private, national and local healthcare providers regulated by DOH and Philippine Health Insurance Corporation

(PhilHealth); national and local public health authorities; DOH partner agencies involved in the collection and processing of COVID-19-related data; all COVID-19 cases; and all individuals identified as close contacts.

IV. DEFINITION OF TERMS

For the purpose of this Joint Memorandum Circular, the following terms are defined:

1. **Anonymization** is a process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party. (ISO/IEC 29100:2011)
2. **Case** refers to an individual who is either a COVID-19 suspect, probable, or confirmed patient.
3. **Close contact** – a person who may have come into contact with the probable or confirmed case two days prior to onset of illness of the confirmed COVID-19 case (use date of sample collection for asymptomatic cases as basis) until the time that said cases test negative on laboratory confirmation or other approved laboratory test through:
 - a. Face-to-face contact with a probable or confirmed case within 1 meter and for more than 15 minutes;
 - b. Direct physical contact with a probable or confirmed case;
 - c. Direct care for a patient with probable or confirmed COVID-19 disease without using proper personal protective equipment; OR
 - d. Other situations as indicated by local risk assessments.
4. **COVID-19-related data** refers to all types of information related to COVID-19 disease surveillance and response, including personal health information of COVID-19 cases and identified close contacts.
5. **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)
6. **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)
7. **Data Subject** refers to an individual whose personal information is processed. (DPA)
8. **Healthcare Providers** refer to any of the following:
 - a. **Health care professional** refers to doctor of medicine, nurse, midwife, dentist, or other skilled allied professional or practitioner duly licensed to practice in the Philippines; and
 - b. **Health facility** refers to a public or private facility or institution devoted primarily to the provision of services for health promotion, prevention, diagnosis, treatment, rehabilitation and palliation of individuals suffering from illness, disease, injury, disability, or deformity, or in need of medical and nursing care.
9. **DOH partner agency** refers to a DOH-designated/deputized public health authority to collect and process COVID-19-related data for purposed specified under Section V.2. of this Guidelines.
10. **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)
- 11. Personal 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-PhilHealth Joint Administrative Order No. 2016-0002)
- 12. 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)
- 13. 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)
- 14. Processing** refers to any operation or any set of operations performed upon patient's data including, but not limited to, the collection, recording, organization, storage, updating or modification, extraction, retrieval, consultation, use, consolidation, blocking, submission, disclosure, erasure or destruction of data. (DPA)
- 15. Pseudonymization** refers to replacing one attribute (typically a unique attribute) in a record by another. The natural person is therefore still likely to be identified indirectly; accordingly, pseudonymization when used alone will not result in an anonymous dataset. (Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques).
- 16. Public Health Authority** refers to the DOH, specifically the Epidemiology Bureau, Disease Prevention and Control Bureau, Bureau of Quarantine, Food and Drug Administration, Regional Offices of DOH, Regional Epidemiology and Surveillance Unit (RESU), local health offices (provincial, city, or municipality); or any person directly authorized to act on behalf of the DOH or the local health office. (DOH Administrative Order [AO] 2020-0013)

V. GENERAL GUIDELINES

1. The implementation of COVID-19 disease surveillance and response shall promote public health action to contain and/or prevent the spread of COVID-19 and help mitigate the effects and impact of the disease to the people and communities, while safeguarding the data privacy rights of every individual.
2. The processing of personal health information of COVID-19 cases and identified close contacts for disease surveillance and response shall be to the extent necessary for the following purposes:
 - a. To outline a true picture of the country's COVID-19 health situation in terms of status and extent of local and community transmission.
 - b. To build a repository of real-time COVID-19-related data as basis of evidence-informed health policy and intervention measures.
 - c. To support case investigation and management, contact tracing and monitoring, quarantine and isolation, mandatory reporting to national and local public health authorities, and other disease surveillance-related activities.
 - d. To improve response activities, including the quality and accessibility of health services and other related interventions for COVID-19.
 - e. To allow information sharing and exchange between and among healthcare providers, public health authorities and other government authorities for treatment and care coordination, and/or surveillance and response purposes.
3. The right to privacy of health information shall be protected at all times. The processing of personal health information of COVID-19 cases and identified close contacts shall be in accordance with RA 10173, its IRR and other relevant issuances from the NPC, and shall adhere to the principles of transparency, legitimate purpose, and proportionality:
 - a. Patients/close contacts (data subjects) 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 involve only the minimum extent of personal data necessary to the declared and specified purpose at the time of collection.
4. All national and local public health authorities, concerned healthcare providers and DOH partner agencies involved in the collection and processing of COVID-19-related data shall put in place the minimum organizational, physical and technical security measures and standards for data protection as set by NPC and the Department of Information and Communications Technology (DICT), and shall uphold and protect the data privacy rights of every individual at all times.
5. This policy shall serve as the privacy notice of national and local public health authorities, and DOH partner agencies in the collection, processing, and disclosure of COVID-19-related data in pursuit of disease surveillance and response.

VI. SPECIFIC GUIDELINES

A. Implementation Governance

1. The Interagency Task Force for the Management of Emerging Infectious Diseases – Task Group on Strategic Communications, in coordination with the DOH –

Epidemiology Bureau, the DOH Data Protection Officer and the National Privacy Commission, shall set policy directions and oversight on all matters relating to privacy and data protection of COVID-19-related data.

2. The National eHealth Program Management Office (NEHPMO) in KMITS of the DOH shall act as the overall technical and administrative secretariat for all activities related to ensuring privacy and data protection of COVID-19-related data.

B. Processing of Health Information

1. The processing of personal health information of COVID-19 cases and identified close contacts shall be allowed in any of the following cases:
 - a. The processing of personal health information is done by national and local public health authorities, pursuant to its constitutional or statutory mandate as provided under RA 11332, Sections 4(e), 12 and 13 of RA 10173, and other applicable laws, rules, and regulations.
 - b. The processing of personal health information by a healthcare provider is allowed if necessary for the purposes of case investigation and management, contact tracing and monitoring, quarantine and isolation, mandatory reporting to public health authorities, or treatment and coordination purposes.
 - c. The processing of personal health information by DOH partner agencies and their authorized personnel shall be allowed, pursuant to a Data Sharing Agreement (DSA) as provided under NPC Circular 16-02 (Data Sharing Agreements Involving Government Agencies).
 - i. All personnel who will be authorized by the DOH partner agencies to collect and process personal health information shall sign a Non-Disclosure Agreement (NDA) beforehand to prevent any unauthorized processing.
 - d. Personal information are pseudonymized or anonymized.
2. In the processing of personal health information, the following must be observed:
 - a. In all cases where processing of personal health information is allowed, the patient/close contact (data subject) shall be informed of the nature and purpose for the collection and processing of his/her personal health information by public health authorities and the DOH partner agencies, which shall include the purposes specified under Section V.2.
 - b. The manner of processing of personal health information shall be in accordance with the guidelines set forth under DOH AO 2020-0013 (Revised AO 2020-0012 "Guidelines for the Inclusion of COVID 19 in the List of Notifiable Diseases for Mandatory Reporting to the DOH dated March 17, 2020), and the DOH DM 2020-0189 (Updated Guidelines on Contact Tracing of Close Contacts of Confirmed COVID-19 Cases).
 - c. Personal health information of all COVID-19 cases and close contacts as identified by concerned healthcare providers, public health authorities and DOH partner agencies during the conduct of respective case investigation and contact tracing must be reported to the DOH and its designated/deputized public health authorities serving as partner agencies.

C. Access of Health Information

1. Only concerned healthcare providers, public health authorities, and DOH partner agencies and their authorized personnel shall be allowed to access the personal health information of the COVID-19 cases and/or identified close contacts, pursuant to the guidelines set forth under DOH AO 2020-0013, and the DOH DM 2020-0189.

2. All entities and individuals with access to the personal health information shall be bound by legal duty to protect the personal health information pursuant to this Guidelines.

D. Use and Disclosure of Health Information

1. The use of personal health information by national and local governments shall be limited to the purposes specified under Section V.2.
 - a. All concerned healthcare providers, public health authorities, and DOH partner agencies and their authorized personnel shall be responsible for limiting the use of personal health information stored within their location to the purpose specified at the time of collection.
 - b. Use for other purposes not indicated under Section V.2. shall be prohibited.
2. Disclosure of personal health information shall be limited to authorized entities, officers, personnel and concerned individuals only, pursuant to the purposes specified under Section V.2.
 - a. Disclosure to the public, the media, or any other public-facing platforms without the written consent of the patient or his/her authorized representative or next of kin, shall be prohibited.
 - b. Any disclosure by the national and local public health authorities to third parties shall be embodied in a DSA.
 - c. The DOH partner agencies must first secure the written consent of the DOH before they can disclose any personal health information to third parties, and the said disclosure shall likewise be embodied in a DSA.
3. The following information may be disclosed for a legitimate purpose:
 - a. Aggregate health information, or pseudonymized or anonymized detailed health information for public communication; and
 - b. Mandatory reporting requirements, including personal health information, to national and local public health authorities, and DOH partner agencies.

E. Use of Information and Communications Technologies (ICTs) for Collection and Processing of Health Information

1. All ICT solutions and technologies used for collection and processing of personal health information of COVID-19 cases and/or identified close contacts shall be registered to the NPC, and comply with the DOH COVID-19 surveillance and response protocols and data requirements.
2. All entities who are interested to develop and implement ICT solutions and technologies for COVID-19 surveillance and response should be registered to the NPC, and follow the minimum ICT standards set by DICT and Knowledge Management and Information Technology Service (KMITS) of the DOH.

F. Business Intelligence and Health Research

1. Only aggregate health information or pseudonymized or anonymized detailed health information shall be shared by public health authorities to stakeholders for the purpose of business intelligence and policy and biomedical researches.
2. All policy and biomedical researches related to COVID-19 surveillance and response shall secure an Ethics Board approval prior to implementation.

VII. ROLES AND RESPONSIBILITIES

A. Data Subjects (COVID-19 Cases, Close Contacts, and Other Informants)

1. Owner of the data.

2. Disclose truthful and accurate information regarding their health condition and exposure to public health authorities and/or DOH partner agencies.

B. Department of Health

1. Provide policy directions and oversight, together with NPC, on all matters relating to privacy and data protection, and processing and disclosure of COVID-19-related data.
2. Evaluate, monitor and direct activities relating to processing and disclosure of COVID-19-related data in pursuit of surveillance and response as provided under RA 11332, its IRR, and other issuances from the DOH.
3. Observe and comply with RA 10173, its IRR, and other issuances from NPC in the processing and disclosure of COVID-19-related data as a personal information controller.

C. National Privacy Commission

1. Provide policy directions and oversight, together with DOH, on all matters relating to privacy and data protection, and processing and disclosure of COVID-19-related data.
2. Evaluate, monitor and direct activities relating to privacy and data protection of COVID-19-related data in pursuit of surveillance and response as provided under RA 10173, its IRR, and other issuances from NPC.

D. Healthcare Providers

1. Report to the DOH and its designated/deputized public health authorities personal health information of identified COVID-19 cases and/or close contacts.
2. Act as personal information controller.
3. Comply with the DOH COVID-19 surveillance and response protocols and standards, including guidelines on privacy and data protection, and processing and disclosure of COVID-19-related data.

E. Public Health Authorities

1. Act as personal information controller.
2. Comply with the DOH COVID-19 surveillance and response protocols and standards, including guidelines on privacy and data protection, and processing and disclosure of COVID-19-related data.

F. DOH Partner Agencies (including Local Government Units)

1. Report to the DOH personal health information of identified COVID-19 cases and/or close contacts.
2. Protect and preserve identities of COVID-19 cases and identified close contacts, and their families to the extent that this does not result in undue discrimination, or physical or emotional harm or distress.
3. Act as both personal information controller and processor.
4. Comply with the DOH COVID-19 surveillance and response protocols and standards, including guidelines on privacy and data protection, and processing and disclosure of COVID-19-related data.

VIII. PENALTY CLAUSE

1. Non-cooperation of any individual to disclose truthful and accurate information regarding their health condition and exposure to COVID-19 to public health authorities and/or DOH partner agencies, or of any individual or entity that should report and/or respond to COVID-19 surveillance and response, or any similar action insofar as they relate to the provisions of

this Joint Memorandum Circular shall be penalized in accordance with RA 11332 (Mandatory Reporting of Notifiable Diseases and Health Events of Public Health Concern Act), RA 11469 (Bayanihan to Heal as One Act), and other applicable laws, rules and regulations.

2. Any privacy violation, or personal data breach, or security incident shall be penalized in accordance with RA 10173 (Data Privacy Act of 2012), or other applicable laws, rules, and regulations. Exemptions for privacy violation include disclosures of personal health information that is publicly known or becomes publicly known for causes not due to any unauthorized act of any concerned implementer of these Guidelines, or public disclosure made by the data subject himself/herself.

IX. REPEALING CLAUSE


All previous issuances that are inconsistent with any provisions of this Joint Memorandum Circular are hereby amended, modified, or repealed accordingly.

X. SEPARABILITY CLAUSE

In the event that any provision or part of this Joint Memorandum Circular is declared unauthorized or rendered invalid by any court of law, those provisions not affected by such declaration shall remain valid and in effect.

XI. EFFECTIVITY

This Joint Memorandum Circular shall take effect immediately.


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


RAYMUND E. LIBORO
Privacy Commissioner and Chairman
National Privacy Commission