Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-068

20 November 2018

[redacted]

Re: PROCESSING OF ANONYMIZED PERSONAL DATA BY ELECTRONIC MEDICAL RECORDS PROVIDER

Dear [redacted]

We write in response to your request for an advisory opinion which sought clarification on whether consent is required for processing of anonymized data through an electronic medical records system for research purposes.

You mentioned in your inquiry that a certain Electronic Medical Records (EMR) provider offers the platform to the healthcare provider at no financial cost. In exchange of the free use of the system, the EMR provider will be using the information encoded and stored by the patient or the representative of the healthcare provider for medical research purposes. The personal information collected by the system includes the physician and patient name, address, email address, telephone number and images.

The privacy notice of the EMR provider posted on their website likewise states that it will collect medical information derived from the practice including the symptoms, test results, diagnoses, prescriptions and treatments. Moreover, the EMR provider intends to anonymize the personal data stored in their system and use it for research purposes.

Scope of the Data Privacy Act of 2012

The Data Privacy Act of 2012[1] (DPA) applies to the processing of any type of personal data by any natural and juridical person involved in the processing of personal data.

Processing involves a wide set of operations performed upon personal data, including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.[2] Thus, the collection, recording, storage and use of the personal data being encoded by the patients and physicians are processing activities as defined above.

[1] An Act Protecting Individual Personal Information In Information And Communications 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] Republic Act No. 10173 (2012).
[2] *Id*. § 3 (j).

5th Floor, Delegation Building, PICC Complex, Vicente Sotto St., Pasay City
URL: https://privacy.gov.ph Email Add: info@privacy.gov.ph

The subject of the processing activities performed by the EMR provider covers both personal information and most importantly, sensitive personal information[3] since it includes the health information of the patient. With this, a higher degree of protection and security is required from personal information controllers (PIC) and personal information processors (PIP). They need to satisfy any of the conditions provided for in Section 13 of the DPA to be able to lawfully process sensitive personal information.

Anonymization of personal data

Information is anonymous when such information "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[4]

We note also that ISO/IEC 29100 defines anonymization as 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.[5]

Any information is considered anonymized if there is no possible means to identify the data subject,[6] that is, the PIC and/or any other person are incapable of singling out an individual in a data set, from connecting two records within a data set (or between two separate data sets) and from any information in such dataset.[7]

However, removing some identifiers, such as patient and physician names, contact information, and location, may not be enough to ensure that the PIC and/or any other person can no longer identify the data subject. Anonymization may necessitate additional measures to guarantee that the anonymity of the information is irreversible.

Electronic Medical Records Systems Provider; Legitimate Purpose; Anonymization Process; Use of Information for Medical Research Purpose

We understand that healthcare providers, as PICs, may subcontract the processing of their medical records to EMR providers. Generally, the EMR provider processes personal data, including medical information of patients and retains it in the system. As PIPs, the EMR providers' role is to process personal data based only on the instructions and purposes of the healthcare providers.

In this particular case, the EMR provider intends to anonymize the personal data outside the primary purpose of the healthcare providers, which is for medical treatment.

[3] Data Privacy Act, § 3 (l).
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119), Recital 26.
[5] ISO/IEC 29100:2011(en), Information technology — Security techniques — Privacy framework, available at https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en
[6] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, §2.1 – Definition in the EU legal context
[7] *Id.*

When the EMR provider goes over and beyond the instructions and purpose of processing intended by the PIC, the healthcare provider, the EMR provider is then acting as a PIC with its own purpose – medical research.

While the EMR provider claims that only anonymized information will be accessed, they should clarify the anonymization process. If before, during, and even after the anonymization process, the EMR provider will have direct access to the original data set that still contains personal data, then the said processing will not be exempt from provisions of DPA and its implementing rules and regulations, considering that at any given time, the EMR provider may connect the relevant data sets.

Consequently, the EMR provider as PIC will be required to comply with any of the criteria for processing under the Sections 12 and/or 13 of the DPA.

In connection with the foregoing, when using personal data for medical research purpose, the processing should comply with the requirements of applicable laws, regulations, or ethical standards, including but not limited to obtaining an informed consent from the patient.

There is a need to clarify first whether the information is truly anonymized before we can confirm that consent is not necessary. If there is any doubt on the anonymity of the information, it is best that consent is obtained.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman