Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2019-036[1]

3 July 2019

[redacted]

Re: COLLECTION AND USE OF PATIENT CASE NUMBER AND APPOINTMENT OF COMPLIANCE OFFICER FOR PRIVACY

Dear [redacted],

We write in response to your inquiry which sought to clarify matters regarding the requirements of the Data Privacy Act of 2012[2] (DPA) vis-à-vis the collection and use of patients' case numbers for the Philippine Obstetrical and Gynecological Society (Foundation), Inc. (POGS) Nationwide Statistics System (PNSS) and as a requirement for doctors applying for eligibility to take diplomate examinations.

In addition, you sought to clarify if POGS can appoint compliance officers for privacy (COPs) in its eleven (11) Regional Chapters, in lieu of data protection officers (DPOs).

POGS Nationwide Statistics System (PNSS); National Census Project; patients' case numbers; requirements for diplomate examinations; proportionality

We understand that POGS has a National Census Project which involves a nationwide electronic census platform using the PNSS deployed in POGS-accredited hospitals. The project involves two applications developed by LeapFroggr (LF): (a) census application and (b) cloud portal to aggregate and generate reports on the anonymized data collected by the census application.

We understand further that POGS will have an outsourcing agreement with hospitals to share the counts or number of incidents of the following, among others:

- OB diagnosis

[1] Tags: personal information controller, personal information processor, proportionality, data sharing agreement, outsourcing agreement, compliance officer for privacy
[2] 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).

- Delivery information
- Neonatal information
- Pediatric age/weight and congenital anomalies
- Gyne diagnosis
- Procedures related to the cases mentioned
- Obstetric and gyne mortality counts and causes

For purposes of accuracy and reliability, the Board of Trustees of POGS suggested the inclusion of the patients' case numbers in the data to be transmitted by the hospitals as this will attest to the transmitted number of counts as true and correct. In addition, POGS will be able to use the case numbers to verify the authenticity of the submitted requirements of doctors applying for diplomate examinations.

Scope of the DPA; personal information; statistical, aggregated data; lawful processing

The DPA applies to the processing of all types of personal information by any natural and/or juridical person involved in personal information processing.[3] The law defines personal information as any information whether recorded in a material form or not, from which the identity of an individual is apparent or can reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[4]

Hence, aggregate or statistical data are not considered as personal information under the DPA since such data cannot identify an individual.

We understand that LF's cloud portal will be used to aggregate and generate reports on the anonymized data collected by the census application. As such, the data that will be processed will be de-identified. Thus, what was previously considered personal and sensitive personal information (collectively, personal data) will be rendered anonymous. Therefore, as previously mentioned, these statistical, aggregate, and de-identified datasets are no longer personal information as defined in the DPA, hence, outside the scope of the law.

However, with the inclusion of the case numbers, the collected information will fall within the purview of personal data since it will be possible to ascertain the identity of each patient.

As such, its processing shall be subject to the provisions of the DPA, making it imperative for data subjects to be notified that personal data pertaining to him or her are being or have been processed, pursuant to their right to be informed. Likewise, data subjects' consent must be obtained prior to collection and use of their data, unless the processing of such personal data will fall under any other criteria for lawful processing under Section 13 of the DPA.

General data privacy principles; privacy by design and default

In developing and implementing the National Census Project, POGS must be mindful of the provisions of the DPA and its Implementing Rules and Regulations (IRR), specifically on adhering to the general data privacy principles of transparency, legitimate purpose and

[3] *Id.* § 4.
[4] *Id.* § 3 (g).

proportionality, implementing reasonable and appropriate organizational, physical, and technical security measures, and upholding data subjects' rights.

As such, POGS must integrate privacy and data protection in all processing activities of the National Census Project, considering the nature of the personal data that requires protection, the risks to the rights and freedoms of the patients as data subjects, current data privacy best practices, among others.[5]

As for the purpose of verifying the authenticity of submitted requirements for diplomate examinations, we refer you to NPC Advisory Opinion No. 2018-016, where a hospital asked for guidance on the issue of submitting reports on the actual cases handled by resident physicians for diplomate board exam and accreditation, to wit:

> "CMC's disclosure of the patients' data for purposes of fulfilling the resident physicians' submission requirements for diplomate board exam and accreditation to the PCS and POGS may be allowed under the DPA provided that the patient has provided consent.
>
> The NPC understands that patients' personal data are necessary in order to avoid fraud cases. An option to consider is to pseudonymize the patients' data prior to disclosing the same. Pseudonymization consists of replacing one attribute (typically a unique attribute) in a record by another. While pseudonymization lessens the risks, personal data which have undergone pseudonymization remains to be personal data, hence, consent is still necessary.
>
> In the event that the CMC can no longer obtain consent from the patients, there should be design methods and techniques wherein the PCS and POGS can validate that the cases handled by the resident physicians are true and correct without involving disclosure of personal data to the said professional societies. This may be in form of a certification from the CMC."[6]

From the foregoing, patients' case numbers need not be collected by POGS as the purpose of the processing could be fulfilled by other means, such as a certification from the respective hospitals that the submitted requirements of doctors for diplomate examinations are true and correct.

POGS may likewise consider alternatives in the processing of the census data and verifying the authenticity of submitted requirements for diplomate examinations vis-à-vis the patients' case numbers, i.e. implementing pseudonymization,[7] having the verification process done at the hospital level before the transmission of data to the cloud portal, etc.

Data sharing; outsourcing; data sharing agreement

As defined in the IRR, data sharing pertains to the disclosure or transfer to a third party of personal data under the custody of a personal information controller (PIC) or a personal information processor (PIP) wherein such transfer was directly instructed by the PIC. The data

[5] See: Data Privacy Act of 2012, § 20.
[6] National Privacy Commission, NPC Advisory Opinion No. 2018-016 (April 12, 2018), citing the Data Privacy Act of 2012, Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, and the EU General Data Protection Regulation, Recital 26.
[7] See: National Privacy Commission, NPC Advisory Opinion No. 2018-029 (June 6, 2018).

sharing agreement then refers to the contract which contains the terms and conditions of a dating sharing arrangement between two or more PICs.[8]

On the other hand, Section 3(d) of NPC Circular No. 16-02 defines outsourcing as the disclosure or transfer of personal data by a PIC to a PIP, while an outsourcing agreement pertains to the disclosure or transfer of personal data by the PIC to a PIP in order for the latter to process the data according to the instructions of the controller.[9]

With this, there is a need to clarify the roles of POGS, LF, and the hospitals in order to determine the obligations and responsibilities of the parties under the DPA, its IRR, and issuances of NPC, since there are two key differences that exist between data sharing and outsourcing.

First, all parties to a data sharing agreement are considered as PICs under the law. In a subcontracting or outsourcing agreement, there has to be at least one PIC and one PIP. Second, in terms of purpose or objective, each party to a data sharing agreement has its own reason for processing the personal data involved, while in a subcontracting or outsourcing agreement, a PIP has no other purpose or objective for processing the personal data other than that imposed by the instructions of the PIC.[10]

POGS and LF may enter into an outsourcing or subcontracting agreement as it is commonly understood, and not necessarily as described under Sections 43-45 of the IRR of the DPA, if LF will not be processing any personal data for POGS in the course of the development of the applications and provided that LF will not be using the data for its own purpose. It likewise follows that there is no need for a data sharing agreement as defined above.

As to the POGS-accredited hospitals, we understand that the data to be shared by them are anonymized data. It is understood that 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."[11]

The sharing of such anonymized data is not an outsourcing activity as contemplated in the definition above. Hence, such sharing arrangement for the anonymized data may be covered by an appropriate contract as determined by the parties. However, if the hospitals will be sharing personal data to POGS, the proper contract to execute is a data sharing agreement.

Appointment of a compliance officer for privacy (COP)

We understand that each of the Regional Chapters of POGS is a separate juridical entity registered with the Securities and Exchange Commission (SEC). Nonetheless, programs of the Regional Chapters are aligned with the purposes and projects of the POGS National Office, and regional activities are subject to the approval of the National Board of Trustees.

[8] National Privacy Commission, NPC Advisory Opinion No. 2017-57 (October 3, 2017).
[9] National Privacy Commission, NPC Advisory Opinion No. 2017-008 (January 9, 2017).
[10] *Id.*
[11] 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) Official Journal of the European Union, Vol. L119, Recital 26 (4 May 2016).

As provided for in NPC Advisory No. 2017-01,[12] PICs in the private sector may designate COPs, subject to the approval of the NPC and the provisions of said Advisory. Specifically, a group of related companies may appoint or designate the DPO of one of its members to be primarily accountable for ensuring the compliance of the entire group with all data protection policies. Where such common DPO is allowed by the NPC, the other members of the group must still have a COP.

Under this scenario, the POGS National Office's DPO may be appointed or designated as a common DPO, and each of the Regional Chapters shall have their COPs. The request for approval of the designation of a common DPO may be done by writing a letter addressed to the NPC Compliance and Monitoring Division (CMD). For further information on the above, you may contact the NPC CMD at compliancesupport@privacy.gov.ph and 234-22-28 local 118.

This opinion is based on the 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

[12] National Privacy Commission, Designation of Data Protection Officers, Advisory No. 2017-01 [NPC Advisory No. 17-01] (March 14, 2017).