Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-22

19 June 2017

[redacted]

Dear [redacted],

This refers to your query which was received by the National Privacy Commission (NPC) on 12 May 2017. Specifically, you put forward the following inquiries:

1. What are the supporting documents necessary for registration?

2. Who are the personal information controller (PIC), personal information processor (PIP), and data protection officer (DPO) in your organization, and/or how should they be selected?

3. What are the reasons why you need to adopt these policies, so you could convince your board of trustees to approve the request for registration?

Registration of Data Processing Systems

The National Privacy Commission requires those who process personal data to register their data processing systems to the National Privacy Commission by September 9, 2017. The initial step (Phase 1) of the registration will require information on the designation of the institution's Data Protection Officer (DPO). The DPO shall serve as contact person of the institution and he or she will be receiving instructions on completion of the Registration process. Currently, registration requires manual submission of the physical/hard copy of the following documents to NPC at Core G, 3/F GSIS Headquarters, Financial Center, Pasay City:

1. Notarized Registration form; and
2. Any official document (e.g., internal memorandum, certificate, appointment paper), signed by the head of institution or appointing authority, confirming the appointment or designation of the hospital's DPO.

The registration form may be downloaded from the Commission's website (www.privacy.gov.ph). For further concerns relating to the registration of data processing systems, including the documentary requirements thereof, parties may also look to the relevant provisions[1] of the Implementing Rules and Regulations (IRR) of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), for guidance on this subject.

PIC, PIP, and DPO

The terms, "personal information controller" (PIC) and "personal information processor" (PIP) are defined in Sections 3(h) and 3(i) of the DPA, respectively. The PIC refers to the individual or organization who controls how personal data– which includes health records, and personnel files-- are being collected, used, stored, or otherwise processed.[2] The PIP refers to any individual or organization processing personal information for the PIC as part of an outsourcing contract or similar agreement.[3] In the health sector, for example, the hospital, as represented by its Owner or Board, is considered the PIC, whereas, the electronic medical records (EMR) system provider is an example of a PIP.

The DPO is the individual designated by the hospital (PIC) to have the primary function of monitoring compliance with the Data Privacy Act, IRR and related issuances. The NPC recently issued Advisory No. 17-01,[4] which lays down guidelines on the designation or hiring of the Data Protection Officer.

As a summary of the aforementioned advisory, the PIC should consider the following principles in selecting the DPO:

1. The DPO should be knowledgeable on relevant privacy or data protection policies and practices;
2. The DPO should understand the processing operations in the hospital, including laws and regulations that are relevant to the health sector;
3. The DPO should be a full-time employee, or hired based on contract with term of at least 2 years;
4. There should be No Conflict of Interest if the DPO is performing other functions in the hospital; and
5. The hospital should be ready to support the DPO in terms of providing resources and training to allow independent and effective performance of DPO functions.

Rationale

The Data Privacy Act is a law that is intended for the protection of personal data. Healthcare facilities, such as hospitals, process personal and sensitive information of patients contained in

[1] *see*: IRR of RA 10173, §46 and §47.
[2] *See* RA 10173, §3(h).
[3] *See* RA 10173, §3(i).
[4] Available at the website of the National Privacy Commission, privacy.gov.ph

health records. Hospitals are therefore subject to the obligations and requirements of the DPA, its IRR, and other issuances by the NPC, including the designation of the DPO.

In the event of a personal data breach or a privacy complaint from a patient, the hospital, as a PIC, must be able to demonstrate its efforts towards compliance. In the event of a personal data breach, the cost of the breach would be much higher than implementing security measures. The DPA provides penalties for non-compliance, and under the Hospital Licensure Act, one of the grounds for revocation of license of hospitals is the repeated violation of existing law. More than a consideration of possible penalties, those in the health sector should be mindful that the duty of protecting patient privacy is at the core of the relationship between health professionals and patient, and inherent in the duties of hospitals as a provider of care. The DPA has as its objectives the strengthening of systems to prevent harm to patients, and cultivating a culture of privacy that is essential to quality care.

For your reference.

Sincerely,

IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner,
Policies and Planning