Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-056

5 October 2018

[redacted]

Re: WEB-BASED ACCREDITATION SYSTEM FOR HOSPITALS

Dear [redacted],

We write in response to your request for an advisory opinion regarding the Web-based Census and Accreditation System (WebCAS) facility, a system that uses personal information of patients submitted by institutions for purpose of their accreditation as pulmonary fellowship training hospitals. You requested for clarification on how the Data Privacy Act of 2012 (DPA) [1] applies to your arrangement with various hospitals, particularly on the following:

1. Whether the transfer of patient data for accreditation or proof of fulfilment is allowed by the Data Privacy Act of 2012 (DPA);
2. Whether consent from patients is required for inclusion of their personal information in the census or whether this is considered quality management where consent may not be required; and
3. Whether de-identification allows retaining hospital number, age and gender of patients?

[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).

Lawful processing of sensitive personal information

A patient's health information is considered as sensitive personal information under the Data Privacy Act. The DPA views information about a person's health as posing a significant risk to data subjects in case of unlawful or unauthorized processing due to its sensitive nature. In general, the processing[2] of sensitive personal and privileged information are prohibited unless one of the conditions stipulated in Section 13 of the DPA is satisfied. Thus, the transfer of patient data from a hospital to the Philippine College of Chest Physicians (PCCP), and its processing in the WebCAS for accreditation purposes, should rely on one of the conditions for lawful processing under Section 13 of the DPA.

Sensitive personal information may be lawfully processed if "the data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing."[3] Section 13 also provides conditions where consent may not be required for lawful processing. This includes processing for medical treatment purpose, or when necessary to protect the life and health of the data subject or another person and the data subject is unable to physically or legally express consent.

The use of the patient's health information for accreditation and training purpose requires consent from patients. A consent guide is available in the NPC Privacy Toolkit accessible at the NPC website.[4]

The processing in this context is not in the nature of a quality management system where the processing is generally internal to the hospital. In this case, the processing involves the transfer of sensitive personal information under control of the hospital to PCCP, and further processing of the same information by the latter. Second, the PCCP does not have a direct relationship with the patient. Where the hospital processes patient data for its own quality management for the purpose of generating statistical data, the hospital is processing personal information under its control and custody. The DPA recognizes that personal information collected for other purposes may be processed for historical, statistical or scientific purposes.[5] This is seen to be compatible with the primary purpose. On the other hand, the PCCP's collection and access to the health information falls outside a patient's reasonable expectation. The patient, as the data subject, should be fully aware of the purpose, extent, and risks of the said processing.

De-Identification

Alternatively, the PCCP may consider obtaining only de-identified personal data from hospitals. Where statistical or aggregated data has already been generated by the hospital, the information will no longer be considered personal information, and may already be used for various purposes.

---

[2] Data Privacy Act of 2012, § 3 Definition of terms, (j) Processing refers to any operation or any set of operations 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.
[3] Id., §13(a)
[4] See National Privacy Commission, Toolkit, available at https://privacy.gov.ph/wp-content/files/attachments/nwsltr/3rdToolkit_0618.pdf (last accessed Oct. 5, 2018).
[5] Id., §11(f)

De-identification may entail the removal of the following personal information:[6]

- Name
- All geographic subdivisions, including street address, city, ZIP Code
- All elements of dates (except year) for dates that are directly related to an individual, including birth, date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs)
- Social security numbers
- Internet protocol (IP) numbers
- Medical records numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any other unique identifying numbers, characters, or code
- Certificate/license numbers

The purpose of de-identification is to remove identifiers so that the remaining information no longer relates to an identified or identifiable person. The "de-identification" being contemplated in this case, where data about hospital number, age and gender are retained, is more appropriately a process of pseudonymization. The inclusion of the hospital number of patients makes it possible to still link the data set to a particular patient, and thus the information cannot be considered as de-identified. Pseudonymized data is still personal information subject to the provisions of the DPA. The benefit of using pseudonymized data is that it demonstrates proportionality in data processing, where the risks to the data subject are decreased.

In all cases, the processing of the said personal data shall be subject to the compliance with the requirements of the DPA, IRR, NPC issuances and other relevant rules and regulations. There should be adherence to principles transparency, legitimate purpose and proportionality. Patients should be informed about their rights, and how they may exercise such rights. Personal information controllers, such as the hospitals and PCCP, should also implement reasonable and appropriate organizational, technical and physical security measures intended for the protection of personal information against any accidental or unlawful disclosure, as well as against any other unlawful processing.

---

[6] U.S. Department of Health & Human Services, Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, *available at* https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale (last accessed 30 July 2018).

This advisory opinion is rendered based on the questions and information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts. Note that the proposed Memorandum of Agreement between PCCP and the participating training institutions has not been reviewed for purposes of this advisory opinion.

For your reference.

Very truly yours,

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

Noted by:

(Sgd.) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning