Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2019-032[1]

12 September 2019

[redacted]

Re: STORAGE AND SHARING OF ELECTRONIC MEDICAL RECORDS (EMR)

Dear [redacted],

We write in response to your letter request for an advisory opinion which sought to clarify two issues in your company's business operations:

- What data protection measures that your organization may further take involving the storage of personal and sensitive personal information of patients; and
- What measures should be taken in complying with the Data Privacy Act of 2012[2] (DPA) with respect to the sharing of the analysis and anonymized disease and medical treatment information.

As stated in your letter, MedCheck E-Commerce, Inc. (MedCheck) is a healthcare clinical data company specializing in the collection and analysis of Real World Evidence (RWE), through a cloud-based EMR software, for non-communicable diseases. This is done through working with medical practitioners and researchers to digitally automate the collection of medical data which can be used to produce data registries and research findings to improve patient care.

We understand from your letter that medical record information entered by physicians and their staff into the system are stored by MedCheck in a cloud-based system. Medical records include personal and sensitive personal information, such as medical information about the patient and the assessment made by the respective physician on disease diagnosis and recommended treatment/s. MedCheck then encrypts and anonymizes the same and subsequently stores

[1] Tags: electronic medical records; anonymization; security measures
[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 Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 13 (a) (2012).

patients' personal information and unidentifiable medical statistics into two separate servers which are both encrypted at rest.

We likewise understand, as per your representation, that MedCheck's business model is focused on aggregating the anonymized medical statistics, specifically anonymized disease and treatment data, from its physicians' practices. Collection of such data is made with the consent of the physicians and is aimed at providing the medical community with medical statistics to improve healthcare practice, such as but not limited to, free access to medical statistics and the creation of databases and health registries.

MedCheck as a personal information controller (PIC)

The DPA defines a PIC as an organization which controls the collection, holding, processing or use of personal information.[3] A personal information processor (PIP), on the other hand, is a juridical person to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject.[4]

If MedCheck serves as an EMR Provider, limited to providing a platform for physicians to process health information for medical treatment purpose, then MedCheck for this particular activity is acting as a Personal Information Processor (PIP). It is clear, however, that data collected by the respective physicians from its patients through the system provided by MedCheck, will be further processed by MedCheck with the intent of using it for statistical and research purposes.

In fact, the data transferred to MedCheck is personal data for anonymization. To the extent that MedCheck has control over the further processing of personal data of the patients, specifically health data, it is acting as a Personal Information Controller (PIC). It is therefore subject to the obligations of a PIC under the DPA such as processing personal data when lawfully allowed,[5] ensuring that reasonable and appropriate safeguards are implemented to protect personal information against any accidental or unlawful destruction, alteration and disclosure, and any other unlawful processing,[6] and upholding data subjects' rights, among others.

Consent of the patients; other lawful criteria for processing

The DPA considers medical and health information as sensitive personal information. Thus, the transfer of patients' medical and health information from a hospital to MedCheck for its further processing, i.e. storage, anonymization, research and/or statistical purposes, requires the consent of the patients.

We understand that 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, unless the processing may be justified by some other lawful criteria provided for under the DPA.

[3] Data Privacy Act of 2012, § 3 (h)
[4] *Id.* § 2 (n).
[5] *Id.*, § § 12-13.
[6] *Id.* § 20.

It is also worth noting that the data subjects should also be informed on how their data shall be processed. For example, details on how the process of anonymization shall be done, how the data shall be stored, risks involved in the said processes, the safeguards MedCheck has in place to minimize the risks, etc. should be provided.

Additional security measures MedCheck should take regarding the storage of personal data

In the processing personal data, reasonable and appropriate organizational, physical and technical measures must be established by MedCheck to secure its storage.[7] This is pursuant MedCheck's obligation as a PIC to uphold the confidentiality of the personal data and the rights of the data subjects at all times.

We understand that MedCheck continuously encourages its physicians and medical practitioners to register their practice with the National Privacy Commission (NPC) and comply with the DPA and MedCheck's data protection policies.

In addition, MedCheck should have technical security measures which may come in the form of policies, procedures, controls, technology and equipment to protect the organization's systems processing personal data. Specifically, the Implementing Rules and Regulations (IRR) of the DPA provide that such measures shall include the following:

a. A security policy with respect to the processing of personal data;
b. Safeguards to protect computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through electronic network;
c. The ability to ensure and maintain the confidentiality, integrity, availability and resilience of their processing systems and services;
d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against incidents that can lead to personal data breach;
e. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
f. A process for regularly testing, assessing, and evaluating the effectiveness of security measures; and
g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.[8]

While security measures may not completely eliminate the risks involved in data processing, these minimize the effects of such risks on the data subjects.

Accordingly, MedCheck should be transparent to the data subjects on how these risks shall be addressed and its capacity as a PIC to address the same. A privacy impact assessment (PIA)[9] on MedCheck's data processing system should be conducted. A PIA shall, among others, assist the

[7] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 25.
[8] *Id.* § 28.
[9] National Privacy Commission, Guidelines on Privacy Impact Assessment, Advisory No. 2017-03 [NPC Advisory 17-03] (July 31, 2017).

organization in the identification, assessment, evaluation and management of the risks involved in the processing of personal data.[10] For a more comprehensive discussion on the conduct of a PIA, kindly refer to NPC Advisory No. 2017-03.

Security measures in the sharing of anonymized medical data and statistics with third parties

We understand that MedCheck is in the business of collection, analysis and sharing of anonymized medical data. For a more comprehensive discussion on the nature of anonymized data, we refer you to NPC Advisory Opinion No. 2017-27 dated 23 June 2017 on Anonymized Data for Marketing Analytics. To reiterate, anonymized data does not fall within the ambit of the DPA.

However, please duly note that the exclusion from the scope of the DPA shall only apply if all the requirements for the anonymization of data have been met. Otherwise, or if there are factors which may possibly identify the data subjects, the sharing of such data must strictly comply with the DPA considering that the processing involves not only personal but also sensitive personal information.

It is also worth noting that MedCheck receives personal data prior to its anonymization. Hence, such data is subject to the provisions of the DPA. We wish to reiterate that in the processing of medical treatment information where the same is not anonymized, the consent, if this is the basis for processing, should be given by the patients themselves and not the physicians. In all cases, patients as data subjects have the right to be informed and notified about the processing of his or her personal data pursuant to Section 16 of the DPA.

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

[10] NPC Advisory No. 2017-03.