Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-081

26 November 2018

[redacted]

Re: ACCESS TO MEDICAL RECORDS IN CR-DR SYSTEM

Dear [redacted],

We write in response to your letter regarding the access, use and destruction of medical records of patients stored in a Computerized Radiography- Digital Radiography (CR-DR) system in relation to the provisions of the Data Privacy Act of 2012 (DPA).[1]

In 2017, Western Visayas Medical Center (WVMC) requested a Special Audit from the Commission on Audit (COA) and pending the result thereof, held in abeyance the amount due to JOSMEF Enterprises (JOSEMEF) for the provision of equipment and system to enhance WVMC's radiography system. Because of this, JOSMEF filed a complaint before the Department of Health (DOH) against the hospital for nonpayment. At the same time, they did not allow the access of hospital personnel to the records of patients contained in the CR-DR System which is owned by JOSMEF. Hence, this inquiry as to whether JOSMEF should allow WVMC access to the data of patients in the CR-DR system, to copy the files, and to require JOSMEF to delete the files from the system should JOSMEF pull out the unit from the hospital.

We note that the concerns raised in this advisory may involve legal issues outside the scope of the DPA, particularly as it relates to interpretation of contracts, contractual obligations between the parties, and adjudication of rights. As we understand, WVMC entered into a joint undertaking with JOSMEF in April 2016 for the latter to provide the former with the equipment and system for the enhancement of its radiography system. We are not in a position to determine the nature of this joint undertaking as this involves not just the legal documents made available to the Commission but a determination of the factual circumstances relevant to the agreement.

Given this, we will only discuss the general principles relevant to this case in so far as such issues may relate to the DPA.

[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).

Personal Information Controller and Personal Information Processor

Given the issue at hand, it is vital to determine the relationship between the two entities in relation to the processing of patient data in the CR-DR System. The rights and obligations of the parties would be different depending on their relationship, particularly if they are joint personal information controllers, or if their relationship is one between a personal information controller and personal information processor. A personal information controller (PIC) refers to the individual or organization who controls how personal data – which includes health records -- are being collected, used, stored, or otherwise processed.[2] On the other hand, a personal information processor (PIP) refers to any individual or organization processing personal information for the PIC as part of an outsourcing contract or similar agreement.[3]

If it were the case that the agreement is strictly for JOSMEF to install, configure and maintain the CR-DR system in accordance with the instructions of WVMC, and for this limited purpose have access to the personal data of patients of WVMC, then WVMC would be considered as the PIC and JOSMEF as the PIP.

It bears stressing that a PIP, as such, does not have a right to control the collection, holding, processing, or use of personal information of data subjects. PIPs must process personal data only in accordance with instructions from or under an agreement with a PIC. Where a PIP performs its own operations upon personal data, such as exercising control over its storage, use or retrieval, the PIP may already be considered a PIC. This means that the PIP will be subjected to all the obligations of a PIC under the DPA, including adherence to the data privacy principles of transparency, legitimate purpose and proportionality. Where a PIP processes personal data for its own purposes, including the retention of records, the PIP may risk liability for unauthorized processing and other DPA violations if the processing is done without consent from data subjects or authority from law.

Principle of Accountability

The principle of accountability is articulated in Section 21 of the DPA, which provides:

> Section 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, **including information that have been transferred to a third party for processing**, whether domestically or internationally, subject to cross-border arrangement and cooperation.
>
> (a) The personal information controller is accountable for complying with the requirements of this Act and **shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. xxx**

Furthermore, Section 14 of the DPA provides that in case the PIC subcontracts the processing of personal information, the PIC is responsible for ensuring that proper safeguards are in place for data protection. This same section also provides that a personal information processor shall comply with all the requirements of the DPA and other applicable laws.

One of the guarantees of the Data Privacy Act is the protection of the rights of data subjects. Under the DPA, the data subject is entitled to the right of reasonable access to contents of his or her

[2] Data Privacy Act of 2012, § 3 (h).
[3] *Id*, § 3 (i).

personal information that have been processed. In this case, this involves ensuring that patients can exercise their right to access medical information relating to them.

In the ordinary course of things, the PIC directly responds to the access requests of data subjects, with the cooperation and assistance of the PIP. The failure of the PIC to uphold the right to access of data subjects, without just and valid grounds, may make the PIC accountable to the data subject. This obligation is similarly imposed on PIPs considered as PICs because they control or determine the means and purposes of processing of personal data.

While the obligation to respond to data subjects rests primarily with the PIC, the PIP to whom a PIC has outsourced the processing of personal data should keep in mind its separate obligation to comply with all the requirements of the DPA. Thus, a PIP would still need to uphold the rights of data subjects. This requirement may be complied with by cooperating and coordinating with the PIC in ensuring that data subjects are able to exercise their rights. Under special circumstances, where the PIC is unable to respond to access requests from data subjects, the PIC may instruct the PIP to put in place mechanisms to directly respond to access requests of data subjects, in order to remain mindful of the rights and interests of the individual about whom personal information is processed.

In this case, this is especially important because denial of access to medical information may impair the rights of patients as data subjects. A medical record is critical to patient care and the restriction or delay of access may have significant implications on the health and life of patients.

While we make no determination on the rights of the parties, the nature of their agreement, or possible liabilities, what is clear is that patients should not be denied access to their medical information. This is part of their rights as data subjects, which must be upheld by both PICs and PIPs.

This opinion is rendered based on the limited 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.) IVY D. PATDU
Deputy Privacy Commissioner
Officer-In-Charge