



Republic of the Philippines  
NATIONAL PRIVACY COMMISSION

**PRIVACY POLICY OFFICE  
ADVISORY OPINION NO. 2017-25**

22 June 2017

[REDACTED]

**Re: EMPLOYER'S ACCESS TO EMPLOYEE'S HEALTHCARE SERVICE USAGE**

Dear [REDACTED],

This refers to your query which was received by the National Privacy Commission (NPC) on 13 June 2017. Specifically, your concern is if your company can be provided a detailed summary of your employees' healthcare service usage. You also raised concern that the Human Resource Office will not be made aware if any employee has a contagious illness that could put at risk other employees.

Under the Data Privacy Act of 2012 (DPA), an individual's health information is classified as sensitive personal information.<sup>1</sup> This means that as a general rule, health information can only be processed if the data subject or patient consents, or if one of the conditions provided in the DPA is met. Section 13 of the DPA provides:

**Section 13. Sensitive Personal Information and Privileged Information.** – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

- (a) 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;
- (b) The processing of the same is provided for by existing laws and regulations: *Provided*, that such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further*, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
- (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

---

<sup>1</sup> RA 10173 §3(l)

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided*, that such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further*, That the sensitive personal information are not transferred to third parties: *Provided, finally*, That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

The fact that a company shoulders the premium for Health Maintenance Organization (HMO) coverage is not one of the conditions contemplated by the law that would justify access of employer to the health information of their employees. In order for the company to have access, it may obtain the consent of the data subject/patient/employee for such purpose.

For purpose of ensuring that an employee does not have a contagious disease or any other illness that could put at risk other employees, the company may implement alternatives to requesting information directly from HMOs. For instance, the company may require that an employee provides a medical certificate showing that he or she is “fit to work” before allowing the said employee to return to work.

These conditions in the preceding paragraphs apply only to the medical record of the employee but it does not extend to information that is not considered sensitive personal information, such as:

1. Summaries of account usage or transaction costs that does not include health information (i.e. medical diagnosis and management details); or
2. Aggregate data or statistical data of healthcare service usage for a given period.

For non-sensitive information, Section 12 of the Data Privacy Act provides for the conditions when personal information (not sensitive personal or privileged information) may be processed without the consent of data subject. These conditions include:

1. Processing of personal information necessary and related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
2. Processing is necessary to comply with a legal obligation;
3. Processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

For guidance, the company should determine what information it requires, and for what purpose will such information be used. Any information requested by the company from the HMO should also be limited to that which is necessary for the purpose of the request. Adequate safeguards to assure confidentiality of such information should also be implemented.

It should be clear that nothing prohibits the company or the employer from asking the employee directly for a medical certificate when necessary for purpose of processing sick leaves, or to avail of benefits and programs, and other legitimate purposes. The company may also secure a valid consent from each employee to access their health information. The company cannot, however, compel an HMO to disclose medical information without authorization from the data subject, or without other legal basis for processing.

HMOs, provider of healthcare services needed by their members, have the duty of strict confidentiality over the sensitive personal information/privileged information that they process. The scope of the Data Privacy Act covers HMOs. They are obliged under the law to adhere to data privacy principles, and implement reasonable and appropriate measures to protect sensitive personal information of their members. The company is likewise covered by the Data Privacy Act and will have the same obligations under the law.

This advisory opinion is based on the limited information provided in the questions, and may vary based on additional information or when the facts are changed or elaborated.

For your reference.

Sincerely,

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