Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2019-010[1]

14 January 2019

[redacted]

Re: ACCESS TO EMPLOYEE 201 FILES AND MEDICAL RECORDS

Dear [redacted],

We write in response to your request for clarification received by the National Privacy Commission (NPC) via email regarding access to employee 201 files and medical records by a company's internal auditor.

We understand that in line with the promotion of the development of a strong corporate governance culture, your company, a publicly-listed corporation, has an Audit Committee that was created to enhance the Board of Directors' oversight capacity over the company's financial reporting, internal control system, internal and external audit processes and compliance with applicable laws and regulations.

The Audit Committee is also responsible, among other functions, for overseeing the Senior Management in establishing and maintaining an adequate, effective and efficient internal control framework. We understand as well that the Audit Committee recommended and approved the creation of an Internal Audit Department as part of their oversight function. The internal auditors, as well as external auditors, are granted independence and unrestricted access to all records, properties, and personnel to be able to perform their respective functions.

The issue at hand is whether internal auditors may be restricted to access the 201 files of employees, given that such records are required for the following procedures:

a. Review of employees requirements if compliant to company policy (including detection of submission of falsified documents, with criminal records, and hiring of unqualified personnel);
b. Review of payroll for re-computation and accuracy of payouts (including unauthorized payouts);
c. Review of Medical Records if really fit-to-work and does not have any communicable disease (the Company belongs to the food industry); and
d. Review of other employee benefits provided to employees related to their home address.

[1] Tags: Access to employee records, 201 Files, Medical Records, Internal Audit

Moreover, you sought clarification on the right of the company to access employee records related to their medical benefits provided by a third-party HMO.

You stated that the HMO sends the company monthly summaries of the amounts of money used by employees in their hospitalization. According to your narration, there are no medical records, hospital billings, itemized hospital charges nor certifications from employees that the amount billed by the HMO is the same amount that was charged to them.

Because of the increase in billings to the company, it is now looking into the possibility of fraudulent padded charges by the HMO, undue hospital charges by the hospital, and unauthorized hospital charges from dependents of employees who are not covered. However, the HMO refuses the company's review of charges because of the Data Privacy Act of 2012.

You now seek clarification on the company's right to inspect medical records, including hospital billings, in the given situation.

Access to 201 files; proportionality

Under Data Privacy Act of 2012[2] (DPA), the processing of personal information is considered lawful when the any of the conditions set in Sections 12 and 13 of the law are met.

The processing of personal information shall be allowed, subject to compliance with the requirements of the DPA and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose and proportionality.[3] The principle of proportionality dictates that the processing of personal information, including collection and access thereto, shall be adequate and not excessive in relation to the declared and specified purpose.

We acknowledge that companies are required to submit reportorial documents to different regulating agencies and bodies including, the Securities and Exchange Commission (SEC), the Bureau of Internal Revenue (BIR), and in the case of publicly-listed companies, the Philippine Stock Exchange (PSE).

To the extent that these reports are required under law or regulation and are necessary for compliance with the company's legal obligation, such processing of personal information of the employees related to the accomplishment of such reports are allowed under the pertinent provisions under Section 12 and 13 of the DPA. Furthermore, reasonable processing of personal information may be allowed to further the company's legitimate interests, which may include the development of a strong corporate governance culture.

In the situation at hand, internal auditors may be allowed access to the 201 files of employees which may contain personal information, only in so far as may be necessary for their functions, which may include the inspection and examination of employee requirements, payroll, and benefits.

Because employees' 201 files may contain sensitive personal information, and thus, access to which must be regulated by institutionalized policies on authority to access. Under Section 20 of the DPA, "a personal information controller must implement reasonable and appropriate

[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 for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] Data Privacy Act of 2012, § 11.

organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing."

In relation to compliance with the provisions of the DPA, its IRR and the issuances of the NPC, the company may look into NPC Circular No. 16-01 on Security of Personal Data in Government Agencies[4] as guidance in the establishment of its policies on security of personal data, including access thereto. While the Circular relates to government bodies and entities, the NPC has used it as a benchmark for best practices in privacy policies in the workplace for the private sector.

Specific to the given situation, the company must establish access controls, particularly granting limited authority to access such 201 files by the Internal Audit Department. In Section 15 of the NPC Circular 16-01, a security clearance to access personal data is required, viz:

> SECTION 16. *Security Clearance*. A government agency shall strictly regulate access to personal data under its control or custody. It shall grant access to agency personnel, through the issuance of a security clearance by the head of agency, only when the performance of official functions or the provision of a public service directly depends on such access or cannot otherwise be performed without such access.
>
> A copy of each security clearance must be filed with the agency's Data Protection Officer.

Thus, the company must institute policies and procedures such as the above for the protection of personal data in its custody.

With respect to medical records, however, access thereto should always be justified as such are classified as sensitive personal information as specifically enumerated under the DPA. Should there be other means to accomplish the purpose, i.e. if the employee is fit to work or does not have any communicable disease, access to the full medical records of the employee may no longer be proportional. The company should consider if fit-to-work certifications would be sufficient. Otherwise, the company should fully inform the employees and seek their consent for access to their medical records.

Consent needed for review of hospital charges

As mentioned, health records are a data subject's sensitive personal information which may not be processed unless the conditions set forth under the DPA are present. In relation to the issue with the HMO's charges, an employee's record of hospital billings, itemized hospital charges, and other medical related expenses, may still be considered as part of his or her health records because these may expose relevant information relating to the employee's health.

The fact that the company shoulders the premium for medical benefits 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 employee for such purpose.[5]

The company may likewise consider asking for a certification from the employees that the amount billed by the HMO is the same as that shown or charged to them.

---

[4] National Privacy Commission, Security of Personal Data in Government Agencies, Memorandum Circular No. 16-01 [NPC Circular 16-01] (October 10, 2016).
[5] See: National Privacy Commission, NPC Advisory Opinion NO. 2017-25 (June 22, 2017).

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