IN RE: COCA-COLA FEMSA PHILIPPINES, INC.
(now Coca-Cola Beverages Philippines, Inc.)
x----------x

NPC BN 18-202

RESOLUTION

NAGA, *P.C.;*

Before the Commission is the Compliance[1] of Coca-Cola FEMSA Philippines, Inc. (CCFPI) (now Coca-Cola Beverages Philippines, Inc.) with the Order of the National Privacy Commission (NPC) through its Complaints and Investigation Division (CID) dated 06 October 2020.[2]

Facts

On 25 October 2018, CCFPI filed its initial breach report before the NPC regarding a data breach involving the Annual Physical Examination (APE) results of its thirty-nine (39) employees.[3] According to CCFPI, it engaged the services of ActiveOne Health, Inc. (ActiveOne), an occupational health services provider, for the periodic medical assessment of CCFPI's employees "to detect in time health risk factors and present ailments derived from the employees' work environment and lifestyle."[4]

In its initial report, CCFPI stated that:

> "ActiveOne provides delivery of the APE through onsite and offsite facilities using its network adjacent to CCFPI's sites. It is also obligated to collect, store and report on employee-patient information and the data collected must be in a format that is transferrable to CCFPI or their future clinical providers taking into account the best practices in the handling of data especially with respect to confidentiality. Moreover, records should be

[1] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc.
[2] *In re: Coca-Cola FEMSA Philippines, Inc.*, NPC BN 18-202, Order dated 06 October 2020.
[3] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at p. 1.
[4] *Id.*, at p. 2.

> coded (using unique identifiers and illness using ICD codes) and entered into an electronic system."[5]

On 24 October 2018, ActiveOne notified CCFPI that some employees of the latter's Carlatan Sales Office requested for their APE results.[6] However, one of ActiveOne's nurses accidentally sent to twenty-five (25) recipients, who are also CCFPI employees, the Microsoft Excel file of the summary of APE results of its 39 employees.[7] The following day, the said nurse tried to recall her email, but failed to successfully recall all of them.[8]

According to CCFPI, there would be a likelihood of unauthorized disclosure of medical conditions of the thirty-nine (39) affected data subjects[9] whose personal data involve their employee numbers, names of the data subjects, personnel areas, company positions, gender, birth date, age, results of laboratory tests, medical check-up remarks and recommendations, and prescribed medications.[10] CCFPI stated that it intended to notify the affected data subjects within the prescribed period.[11]

Lastly, CCFPI's initial report contained statements on the safeguards it implemented to minimize or mitigate the impact of the incident which provide the following:

1. Clinic Operations Manual which provides for the standard APE procedure on the proper disposition and securing the confidentiality of the APE results.
2. ActiveOne's Academy On-boarding Orientation regarding CCFPU Processes which is provided to and required all of its Nurses and Doctors.
3. ActiveOne's Memorandum dated 05 October 2018 addressed to its Nurses and Doctors assigned to CCFPI concerning the Procedure for the Release of Records including APE results.
4. Soon after CCFPI was notified of the breach incident on 24 October 2018, CCFPI recalled the subject email communication of Nurse A and copies thereof were successfully deleted on the recipients' mailboxes.[12]

---

[5] *Id.*
[6] *Id.*
[7] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at p. 2.
[8] *Id.*
[9] *Id.*, at p. 3.
[10] *Id.,* at pp. 3-4.
[11] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at p. 4.
[12] *Id.,* at p. 3.

Moreover, CCFPI also stated its proposed measures to be taken to address the breach which are:

1. Subject Nurse A to disciplinary action under ActiveOne's Employee Discipline Policy.
2. Continuing education for all ActiveOne's Onsite Personnel on Data Privacy Law and ActiveOne's Internal Policies on Medical Data Confidentiality.
3. Include in ActiveOne's Clinic Process Manual a procedure on safeguarding electronic data by encryption.[13]

On 06 October 2020, the NPC's Complaints and Investigation Division (CID) issued an Order requiring CCFPI to submit a Full Report which contains the details provided under Rule V, Section 17 (D) of NPC Circular No. 16-03 (Personal Data Breach Management).[14]

On 18 November 2020, CCFPI moved for a 15-day extension for the submission of its Full Report stating that it is encountering difficulties in coordinating with ActiveOne due to the pandemic[15] which the CID granted in its 20 November 2020 Resolution.[16]

In compliance therewith, CCFPI, now Coca-Cola Beverages Philippines, Inc. (CCBPI) submitted its Full Report dated 03 December 2020 attaching therein documents to substantiate security measures it implemented to address the breach.[17]

Issue

Whether CCBPI sufficiently complied with the Order of NPC dated 06 October 2020.

Discussion

CCBPI sufficiently complied with the Order of NPC dated 06 October 2020. The Commission therefore resolves to close the instant case.

---

[13] *Id.,* at p. 4.
[14] *In re: Coca-Cola FEMSA Philippines, Inc.*, NPC BN 18-202, Order dated 06 October 2020, at pp. 1-2.
[15] Motion for Extension dated 18 November 2020 of Coca-Cola FEMSA Philippines, Inc.
[16] *In re: Coca-Cola FEMSA Philippines, Inc.,* NPC BN 18-202, Resolution dated 20 November 2020.
[17] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc.

I. The incident falls under the mandatory breach notification requirement.

Rule V, Section 11 of NPC Circular No. 16-03 provides:

> **Sec. 11.** ***When notification is required.*** Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:
>
> A. **The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.** For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
> B. There is **reason to believe that the information may have been acquired by an unauthorized person**; and
> C. The personal information controller or the Commission believes that the unauthorized acquisition is **likely to give rise to a real risk of serious harm to any affected data subject**.[18] (Emphasis supplied)

In its initial breach report, CCFPI stated that a nurse from ActiveOne accidentally sent the MS Excel file of the summary of APE results of 39 employees to 25 employees of CCFPI[19] which contained the employee numbers, names of the data subjects, personnel areas, company positions, gender, birthdate, age, results of laboratory tests (i.e. chest x-ray, fecalysis, complete blood count, urinalysis, dental examination, and blood chemistry), medical check-up remarks and recommendations, and prescribed medications.[20]

---

[18] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 11 (15 December 2016) (NPC Circular 16-03).
[19] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at p. 2.
[20] *Id.,* at pp. 3-4.

As defined under the Data Privacy Act of 2012 (DPA), sensitive personal information refers to personal information:

> (1) About an individual's race, ethnic origin, marital status, **age,** color, and religious, philosophical or political affiliations;
>
> (2) About an **individual's health**, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;[21] (Emphasis supplied)
>
> …

Based on the definition, the APE results contained not only the names of the affected data subjects, but also sensitive personal information such as their birthdates, age, gender, and the results of laboratory tests, medical check-up remarks and recommendations, and prescribed medications. [22]

Further, the employee numbers, names of the data subjects, personnel areas, and company positions,[23] are considered other information that may be used to enable identity fraud, such as when a fraudster would identify himself or herself as an employee of CCFPI and whose medical records can be used to avail health care services or products that are covered by company medical programs. Thus, the first requisite of Section 11 of the Circular No. 16-03 is present in this case.

Moreover, CCFPI reported that such APE results were accidentally sent to different recipients other than the affected data subjects.[24] Even though the APE results were sent to employees of CCFPI, the said recipients were unauthorized to acquire the same. Thus, the second requisite is present considering that APE results were acquired by unauthorized persons.

---

[21] 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, chapter I, § 3(l) (2012).
[22] Breach Notification dated 25 October 2018 of Coca-Cola FEMSA Philippines, Inc., at pp. 3-4.
[23] *Id*.
[24] *Id*., at p. 2.

Lastly, CCFPI stated in its initial report that there would be a likelihood of unauthorized disclosure of medical conditions of the affected data subjects.[25] The fact that the email containing the APE results was sent to other CCFPI employees and that the nurse who accidentally sent the same failed to recall such email, the incident may therefore give rise to a real risk of serious harm to the affected data subjects such as identity theft or fraud especially when claiming health care benefits. Thus, the third requisite is present in this case.

Considering that all the requisites under Section 11 of NPC Circular 16-03 are present in this case, CCFPI, as personal information controller, is mandated to notify the affected data subjects to allow them to take "the necessary precautions or other measures to protect themselves against the possible effects of the breach."[26]

However, CCFPI, now CCBPI, already implemented security measures to mitigate the harm and has notified the affected data subjects regarding the incident.

II. CCBPI has security measures in place to mitigate the breach and the recurrence of the incident; CCBPI sufficiently notified the affected data subjects of the breach.

In an Order dated 06 October 2020, the CID required CCFPI to submit a Full Report which contains the details provided under Rule V, Section 17 (D) of NPC Circular No. 16-03.[27] Among those required to submit are the description of the measures taken to address the breach and to recover the personal data that were compromised, actions performed to mitigate the possible harm and those taken to inform the affected data subjects of the breach, and the measures taken to prevent recurrence of the incident.[28]

---

[25] *Id.,* at p. 3.
[26] NPC Circular 16-03, rule V, § 18(A).
[27] *In re: Coca-Cola FEMSA Philippines, Inc.,* NPC BN 18-202, Order dated 06 October 2020, at pp. 1-2.
[28] *Id.*

In its Full Report dated 03 December 2020, CCBPI submitted necessary documents as proof of its compliance.[29]

According to CCBPI's Full Report, there were forty (40) employees whose APE results were inadvertently sent to 25 email recipients who are also employees of CCBPI,[30] causing a disclosure of a total number of six hundred forty (640) personal records.[31]

To minimize or mitigate the harm, it was reported that ActiveOne issued a Memorandum addressed to its nurses and doctors assigned to CCBPI about the process of releasing the records including APE results.[32] CCBPI also attached an affidavit of its former Data Protection Officer stating that "[u]pon receiving the report, [CCFPI] recalled the subject email communication of said nurse and copies thereof were successfully deleted from the recipients' mailboxes."[33]

CCBPI also submitted the affidavits executed by the affected data subjects stating that "[they] did not experience any negative effect or untoward incident due to the mistake committed by the ActiveOne nurse in sending the results of [their] to unintended recipients."[34]

Moreover, as to the measures taken to address the breach, CCBPI reported that ActiveOne subjected the concerned nurse to disciplinary action,[35] and that upon report of the breach, a subsequent investigation was conducted by ActiveOne's management.[36]

CCBPI also reported that ActiveOne conducts continuing education for all its personnel regarding DPA and ActiveOne's internal policies on Medical Data Confidentiality.[37] Further, ActiveOne, as a subsidiary of RellianceCARE, Inc., included in its Data Privacy Manual policies on the technical security measures procedure which include the use of systems to be used as monitoring security for breaches, the evaluation

---

[29] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc.
[30] *Id.,* at p. 1.
[31] *Id.,* at p. 2.
[32] *Id.,* referred to as Annex "A."
[33] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc., at p. 3; referred to as Annex "B."
[34] *Id.,* at p. 2; referred to as Annexes "C" to "C-37."
[35] *Id.,* at p. 4.
[36] *Id.*
[37] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc., at p. 4.

of software applications prior to their installation in their computers or devices, the conduct of vulnerability assessments and penetration testing, and the encryption and authentication procedures it will implement to control and limit access to personal data.[38]

ActiveOne's Data Privacy Manual also provides policies on the physical security measures which contain procedures on data formatting, personal data storage, accessing by company personnel, monitoring and limitation of access to the storage facility, modes of transfer, retention, and disposal of personal data.[39]

To prevent the recurrence of the breach, CCBPI published its own Privacy Manual which contains provisions on security measures it shall implement in order to maintain the availability, integrity, and confidentiality of personal data.[40] As part of its "organizational security measures," CCBPI shall appoint its Data Protection Officer, conduct trainings and seminars regarding data privacy and security, and conduct of the Privacy Impact Assessment (PIA), among others.[41]

Also, as part of its "physical security measures," CCBPI provided procedures on the storage, access, monitoring, and transfer of personal data, among others.[42]

CCBPI's Privacy Manual also contains provisions on the creation of a data breach response team to endure immediate response and appropriate action in case of personal data breach.[43] CCBPI also stated it shall regularly conduct a PIA to identify the risks in the processing system.[44] Lastly, the Privacy Manual of CCBPI also contains a procedure for recovery and restoration of personal data, a notification protocol to the company's management, NPC and the data subjects, and a procedure on the documentation and report of security incidents or personal data breach.[45]

---

[38] *Id.,* referred to as Annex "E," at pp. 24-26.
[39] *Id.,* at pp. 20-23.
[40] *Id.,* at p. 5; referred to as Annex "G," at p. 12.
[41] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc., at p. 5; referred to as Annex "G," at pp. 12-13.
[42] *Id.,* at pp. 13-15.
[43] *Id.,* at p. 18.
[44] *Id.,* at p. 19.
[45] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc., at p. 5; referred to as Annex "G," at pp. 19-20.

Furthermore, CCBPI attached in its Full Report screenshots of a communication released by its Office of Internal Control regarding data labels and electronic mail classification,[46] and of the "Drops of Knowledge"[47] which the CCBPI launched containing Data Privacy trainings used as a mandatory compliance requirement for all CCBPI associates.[48]

Finally, as to the actions taken to inform the affected data subjects, CCBPI was able to promptly notify the 40 employees affected by the breach, as proven by notification letters dated 25 October 2018 sent to them.[49] In the said notification letters, CCBPI explained how the breach occurred, the safeguards it took to minimize or mitigate the risk of the incident, and the actions it implemented and will implement "to decrease the likelihood of a similar incident from happening again."[50] Such action taken to notify the affected data subjects is deemed by the Commission as sufficiently compliant with the mandatory notification requirement and the contents thereof under NPC Circular 16-03.

It is in these types of cases where sensitive personal information and other information that, under the circumstances, may enable identity fraud are involved, the Commission repeatedly reminds the personal information controllers (PICs) and processors (PIPs) of their obligation under the DPA to promptly notify the affected data subjects of a personal data breach[51] in order for them to take necessary actions "to protect themselves against the possible effects of the breach."[52]

Following the principle of proportionality under the DPA and its Implementing Rules and Regulations, the "processing of information

---

[46] *Id.*, referred to as Annex "H."
[47] *Id.*, referred to as Annex "I."
[48] *Id.*
[49] Compliance dated 03 December 2020 of Coca-Cola FEMSA Philippines, Inc., at p. 4; referred to as Annexes "F" to "F-39."
[50] *Id.*
[51] 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, chapter V, § 20 (f) (2012).
[52] NPC Circular 16-03, rule V, § 18(A).

shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose."[53]

Necessarily, to avoid further recurrence of this incident as well as to comply with the proportionality principle, CCBPI's access to its employees' periodic medical assessment should be limited to the physician's evaluation of whether an employee is "fit to work" instead of providing the specific laboratory results of the APE. Such evaluation may be seen in a medical certificate issued to the employees upon their request, as to ensure the confidentiality of the medical records of CCBPI's employees.

WHEREFORE, premises considered, this Commission resolves that the matter on NPC BN 18-202 "In re: Coca-Cola FEMSA Philippines, Inc." is hereby considered **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
19 October 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

[53] 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, chapter III, § 11 (2012); *see also* Implementing Rules and Regulations of the Data Privacy Act of 2012, rule IV, § 18(c) (2016).

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

EB
Data Protection Officer

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission