IN RE: AIG SHARED SERVICES - BUSINESS PROCESSING INC. AND AIG SHARED SERVICES CORPORATION – MANAGEMENT SERVICES (ROHQ) **NPC BN 18-033**

x----------x

IN RE: MEDICARD PHILIPPINES, INC. - FESTIVAL ALABANG CLINIC **NPC BN 18-076**

x----------x

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is the consolidated breach notifications submitted by AIG Shared Services Corporation – Management Services (ROHQ) (AIGSS-MS) by AIG Shared Services – Business Processing Inc. (AIGSS-BPI) (collectively, AIGSS) and by Medicard Philippines, Inc. - Festival Alabang Clinic (Medicard).

Facts

On 12 March 2018, AIGSS-MS notified the National Privacy Commission (NPC) of a breach:

> In accordance with RA. 10173, "Data Privacy Act of the Philippines", this is to notify the Commission of a recent personal data breach that happened in our organization. Unfortunately, **sensitive personal information of one (1) employee was inadvertently sent to unintended recipients by our medical service provider [i.e. Annual Physical Exam (APE) results were sent to all affected data subjects instead of sending it individually].** The full report of the personal data breach will be

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> sent separately. We will also send the acknowledged notification letter by the data subject to you as soon as we receive it.[1]

It attached a Privacy Risk Incident Report (Report) stating that the following personal data of its employees were involved: full name, employee ID, and medical information.[2] AIGSS-MS explained that "human error" was the "principal root cause," and that Medicard was also a responsible party.[3] It stated that the potential harm that may result from the incident was "emotional distress" and "reputational damage."[4] AIGSS-MS reported that it informed the affected data subjects and obtained confirmation from the recipients that the email was deleted and not reproduced.[5] Finally, it reported that it already informed Medicard and was waiting for its response on the matter.[6]

On 14 March 2018, AIGSS-BPI also notified the NPC of the breach.[7]

On 23 May 2018, Medicard submitted its breach notification, stating:

> 1. Nature of the Breach/Incident: Unintended disclosure of Annual Physical Exam (APE) Results
>   a. Appointment Officer voluntarily performed the duty of Records Technician to send APE Results of 6 data subjects the neglecting protocol last March 9, 2018.
>   b. The unencrypted APE Results were sent to unintended recipients within AIG.
> 2. Personal Data Possibly Involved: APE Results
> 3. Remedial Measures to Address the Breach/Incident:
>   a. Deletion of all copies of the email containing unencrypted APE Results.
>   b. Disciplinary action for the Appointment Officer.

---

[1] Personal Data Breach Notification from AIG Shared Services Corporation - Management Services (ROHQ), 12 March 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018). Emphasis supplied.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Personal Data Breach Notification from AIG Shared Services Corporation - Business Processing Inc., 14 March 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> c. Reorientation of all clinic personnel of existing security measures.
> d. Segregation of duties and limit number of clinic personnel who sends APE Results.
> e. Company-wide Data Privacy and Information Security Awareness Program.
>
> Kindly see attachments for the details.[8]

Medicard submitted two email threads to its notification: the first involved the email thread of the breach itself,[9] and the second involved AIGSS and Medicard's correspondence after the breach.[10] AIGSS initiated the correspondence to inform Medicard of the breach.[11] It stated that it was expecting Medicard to perform all measures "to protect [AIGSS'] employees' sensitive personal information."[12] AIGSS also requested an explanation from Medicard, its next steps in addressing the breach, and its assistance in ensuring the email is deleted.[13] Finally, Medicard submitted an email apology sent by Medicard's Alabang Officer to AIGSS.[14]

On the notification of the affected data subjects, Medicard explained:

> We did not perform immediate breach notification because we considered the incident as low/minimal risk and would not cause harm to the 6 data subjects because the recipients of the APE Results were all within AIG. MediCard is committed to complying with RA 10173. We would like to ensure that we are complying with the breach notification requirements even though AIG claimed that they have already reported the breach/incident to the Commission.[15]

---

[8] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018). Emphasis supplied.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[15] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

On 07 August 2018, the NPC, through the Complaints and Investigation Division (CID), directed AIGSS to submit its Full Report within five (5) days from receipt.[16]

On 21 September 2018, AIGSS requested an additional period of seven (7) days, or until 28 September 2018, to submit the Full Report.[17] It explained that it needed additional time because of "[t]he volume and nature of the information that it needs to review, as well as AIGSS's desire to provide [the Commission] a Full Report that is both comprehensive and in full compliance with the Memorandum."[18]

On 28 September 2018, AIGSS submitted its Full Report in compliance with the Memorandum dated 07 August 2018.[19]

AIGSS explained that between 11 February 2018 and 02 March 2018, the Annual Physical Exam (APE) of six (6) AIGSS employees was conducted in the Medicard Festival Alabang Clinic. [20] On 09 March 2018, AIGSS' Human Resources Employee (HR employee) requested scanned copies of the APE results of the six (6) employees from the Medicard Alabang Officer to comply with the Occupational Health Permit requirements due on the same day.[21]

The HR employee asked the Medicard Alabang Officer to send the APE results to the Medicard Nurse based in the AIGSS iHub Clinic (iHub Medicard Nurse).[22] In turn, the HR employee instructed the iHub Medicard Nurse to "encrypt and password protect each APE result before sending it individually" to the six (6) employees.[23] The Medicard Alabang Officer, however, sent all the APE results to four (4)

---

[16] Memorandum, 07 August 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[17] Request for extension, 21 September 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[18] *Id.*
[19] Full Report, 28 September 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[20] *Id.* at 1.
[21] *Id.*
[22] *Id.*
[23] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

out of the six (6) employees, instead of the iHub Medicard Nurse.[24] Further, it was sent without following "the agreed process for handling APE results."[25]

AIGSS stated that on 10 March 2018, one (1) of the four (4) recipient employees reported the incident to the AIGSS Privacy Team.[26] The Privacy Team then initiated a review of the incident and implemented "remediation measures to contain the breach."[27]

The affected data subjects were five (5) employees of AIGSS–BPI and one (1) employee of AIGSS–MS.[28] The following personal information were affected: "1) Full Employee Name, 2) Employee ID Number, 3) Age, 4) [Civil] Status, and 5) Medical Information."[29] AIGSS maintained, however, that other than the AIG Employee ID "there were no other personal information compromised which could enable identity theft."[30]

On measures to address the breach, AIGSS reported that within seventy-two (72) hours, it obtained email confirmation from the four (4) recipients that "the email had been deleted and was not retained or used by them."[31]

On the notification of the affected data subjects, AIGSS reported that it sent an email to the six (6) affected employees to notify them of the incident.[32] AIGSS explained that this was "because they were AIGSS employees at the time the incident occurred."[33]

---

[24] *Id.* at 2.
[25] Full Report, 28 September 2018, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.* at 3.
[30] *Id.*
[31] Full Report, 28 September 2018, at 3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[32] *Id.* at 5.
[33] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

AIGSS also reported sending an email to Medicard on 13 March 2018 "informing them about the incident and demanding for an explanation on why the agreed process for distributing APE results was not followed."[34] AIGSS asked for Medicard's remedial measures to ensure the incident does not occur again.[35] On 15 March 2018, AIGSS reported that Medicard responded and advised AIGSS that it had taken the following remedial measures: refresher training for all Medicard staff, implementation of more stringent protocols to safeguard its clients' sensitive personal information, and reduction or limitation of the number of staff that can access clients' sensitive personal information.[36]

On 13 January 2021, the CID issued an Order to Medicard, directing it to submit a Full Report on the breach notification dated 23 May 2018.[37]

On 02 February 2021, Medicard submitted its compliance with the Order dated 13 January 2021:

> On March 9, 2018, 6:42am, AIG-HR staff Ms. AMB emailed Ms. JL2[sic] (Appointment Officer) of MediCard-Festival Alabang Clinic to send the APE results of 6 employees before 12nn on the same day. From the same email, she then instructed 2 other AIG Personnel (CRN and ihub nurse) to send the said APE results to the 6 employees. At 11:39am of the same day, Ms. JL of MediCard Festival Clinic sent the APE results. However, she included the 6 employees on the said email neglecting the instructions given by Ms. AMB.
>
> On March 10, 2018, 1:18am, upon receiving Ms[.] JL's email, Ms[.] AMB of AIG replied that the APE results were sent to [ ] unintended recipients and that she [was] clear of her instructions that she only authorized CRN and ihub nurse to send the results to their owners and not her.
>
> Ms. JL sent her apologies to Ms. AMB following the incident (email dated March 10, 9:22am) and explained that she thought it was allowed to send the results to the employees since they need to submit it as part of the requirement for their health

[34] *Id.* at 3.
[35] *Id.*
[36] *Id.* at 4.
[37] Order, 13 January 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> permit. She also voluntarily performed the duty of a Records Technician to send the APE results due to the urgency of the request.[38]

Medicard also submitted the following documents with its compliance: a screenshot of Clause 7 from Medicard and AIGSS' contract;[39] an email to AIGSS providing a narration of the breach and the countermeasures it implemented;[40] and a copy of the email thread where AIGSS requested its employees to delete the email.[41]

As proof of the security measures it implemented, Medicard also submitted the following documents: a memorandum from Medicard's Clinic Services Department addressed to all personnel, reminding them of minimum requirements in handling personal and sensitive personal information;[42] a Notice of Disciplinary Action to the Medicard Alabang Officer imposing a ten-day suspension;[43] screenshots of Medicard's internal information campaign on procedures to protect personal information;[44] a memorandum requiring attendance of Medicard employees, contractuals, and consultants to a data privacy and information security awareness training;[45] a memorandum requiring the encryption of digitally processed personal information within Medicard's system; and a memorandum announcing th0e implementation of security features of "Sophos Email Appliance (email gateway)" starting 01 October 2018.[46]

On 26 February 2021, the CID sent another Order to AIGSS, directing it to submit a Full Report on the breach notification in 2018.[47]

---

[38] Full Report, 02 February 2021, at 2-3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] Full Report, 02 February 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[45] *Id.*
[46] *Id.*
[47] Order, 26 February 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

On 11 March 2021, AIGSS filed a Motion for Extension to submit its compliance with the Order dated 26 February 2021.[48] It explained:

> The current deadline you have provided to us to respond to the Order falls on Monday, 15 March 2021 (given that 13 and 14 March fall on the weekend). However, as the matter that is the subject of the Order occurred sometime ago (the matter occurred three years ago and our last correspondence with your good office was in September of 2018), we require further time to collate the information surrounding this matter.
>
> In the circumstances, we are humbly requesting your good office for an extension of time **until 29 March 2021** to respond to your Order.[49]

On 29 March 2021, AIGSS submitted its compliance with the Order dated 26 February 2021.[50] At the outset, AIGSS argued that any investigations by the NPC should be directed at Medicard, who was the PIC of the affected data subjects.[51] It noted that the description of the Order dated 26 February 2021 stated the NPC was investigating "Possible Data Privacy Violations Committed by [AIGSS-BPI] and [AIGSS-MS]."[52] AIGSS explained:

> We believe that any investigations which your good office wishes to conduct in this matter should not be directed at either AIGSS-BPI or AIGSS-MS as we were not the Personal Information Controllers of the personal information found in the results of the annual physical examinations ("APE"). We have explained below that Medicard Philippines, Inc. ("Medicard") was the Personal Information Controller of the APE results. You may, therefore, wish to contact Medicard directly (if not already done) should you have any queries regarding this matter as they will be in the best position to provide you with the relevant information relating to this matter.[53]

---

[48] Motion for Extension, 11 March 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines – Festival Alabang Clinic, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[49] *Id.* at 1.
[50] Compliance, 29 March 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[51] *Id.* at 1.
[52] *Id.*
[53] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

AIGSS then explained that "Medicard is a licensed healthcare provider and Health Maintenance Organization which offers Corporate Health Programs."[54] AIGSS – MS and AIGSS-BPI participated in Medicard's Corporate Health Program "for the purposes of offering employees medical benefits."[55] As part of these medical benefits, employees were entitled to an annual physical examination.[56] According to AIGSS, "six (6) employees (5 from AIGSS-BPI and 1 from AIGSS-MS) attended one of Medicard's own free-standing clinics, the Medicard Alabang Clinic, at Festival Supermall, Alabang, Muntinlupa City between February 11 and March 2, 2018 for their annual physical examinations."[57]

AIGSS then proceeded to discuss the breach, substantially reiterating its narration in the Personal Data Breach Notification.[58] It added that "[t]he APE results were also not meant to be sent directly to the AIG Shared Services Human Resources officer."[59] It clarified that "Medicard ought to have instead sent an email to each of the 6 employees individually, attaching only the APE results of the employee to whom each of the emails was addressed."[60]

AIGSS also reiterated its position that Medicard is the PIC.[61] It stated that the notification to the Commission on 12 and 14 March 2018 was made only "as a courtesy and out of an abundance of caution on behalf of [AIGSS'] employees."[62] It explained:

> 5. [T]he purposes for which Medicard collects, uses, discloses and/or processes the personal information found in the results of APEs as well as the methods used by Medicard in collecting, using, disclosing and processing the said personal information is entirely in the control of Medicard. Medicard provides the APE

---

[54] *Id.*
[55] *Id.*
[56] Compliance, 29 March 2021, at 1-2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[57] *Id.* at 2.
[58] *Id.* at 1-2.
[59] *Id.* at 2.
[60] *Id.*
[61] *Id.* at 1.
[62] Compliance, 29 March 2021, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> results directly to the employees and not to either AIGSS-BPI or AIGSS-MS. In the circumstances, Medicard was the Personal Information Controller in respect of the personal information found in the APE results and was obliged to protect such personal information from, amongst other things, accidental disclosure.
>
> . . .
>
> 7. As AIGSS-BPI and AIGSS-MS were aware of the matter, we informed your good office about the matter through our emails of March 12 and 14, 2018 as a courtesy and out of an abundance of caution on behalf of our employees. For the avoidance of doubt, any obligation to notify your good office of this matter pursuant to the Data Privacy Act of 2012 ("Privacy Act") falls on Medicard as the Personal Information Controller which disclosed the APE results of the 6 employees and not AIGSS-BPI nor AIGSS-MS.[63]

Issue

Whether AIGSS and Medicard were able to sufficiently address the breach and to implement security measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03 (Personal Data Breach Notification). Only the first two requisites are present in this case. The third requisite of real risk of serious harm is absent because of the security measures that AIGSS implemented.

Section 11 of NPC Circular 16-03 provides:

> Section 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.

[63] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

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.[64]

Following this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[65]

The first requisite is present. The information involved is sensitive personal information and other information that may enable identity fraud.

The information inadvertently emailed by the Medicard Alabang Officer includes the employees' age, civil status, and medical information,[66] and Medicard ID number.[67] These are considered

[64] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).
[65] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and Other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-SS-22-001-and-NPC-SS-22-008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 02 August 2023).
[66] Full Report, 28 September 2018, at 3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[67] *Id.* at 3.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

sensitive personal information under Section 3 (l) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA). [68]

Further, the information involved may enable identity fraud, since it may be "made the basis of decisions concerning the data subject, including the grant of rights or benefits."[69] AIGSS stated that "Medicard is a licensed healthcare provider and Health Maintenance Organization which offers Corporate Health Programs."[70] AIGSS–MS and AIGSS-BPI participated in Medicard's Corporate Health Program "for the purposes of offering employees medical benefits."[71] This, taken together with the fact that the information compromised included employee information and Medicard ID number, may enable identity fraud for the purpose of claiming medical benefits.

Medicard also submitted a screenshot of Clause 7 from Medicard and AIGSS' Agreement, which provides:

> **7. AUTHORITY TO EXAMINE MEDICAL RECORDS.** The COMPANY hereby represents and warrants that, at the time of the effectivity of this Agreement and **effectivity of coverage of each MEMBER and his dependents,** it has obtained from the MEMBER and his dependents the required consents authorizing MediCard and any of its authorized representatives to: (a) obtain, examine and process the MEMBER'S personal information, including the medical records of their hospitalization, consultation, treatment or any other medical advice in connection with the **benefit/claim availed under this Agreement;** and (b) disclose such information to the COMPANY and its representatives[.][72]

The use of "dependents" and "benefit/claim" in Clause 7 shows that, apart from providing medical examinations for Occupational Health

---

[68] *See* 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 § 3 (l) (2012).
[69] NPC Circ. No. 16-03, § 11 (A).
[70] Compliance, 29 March 2021, at 1, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[71] *Id.* at 1.
[72] Full Report, 02 February 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Permit requirements, the Agreement between Medicard and AIGSS includes Medicard health insurance coverage for AIGSS employees and their dependents.[73] The name, age, and civil status of the employee, taken together with their employee ID number, are necessary considerations for Medicard's decision to grant medical benefits or claims of AIGSS' employees.

Given the foregoing, unauthorized acquisition of the personal data and APE results may be used to fraudulently assume the identity of an AIGSS employee covered by Medicard's Corporate Health Program.

The second requisite is also present. Unauthorized persons acquired the personal data and APE results in the emailed Excel file.[74]

The Commission held that a loss of control over personal data held in custody is enough for a PIC to have "reason to believe that the information may have been acquired by an unauthorized person."[75]

AIGSS admitted that the Medicard Alabang Officer sent all the APE results in a single email to four (4) out of the six (6) employees, instead of the iHub Medicard Nurse.[76] Medicard reiterated this in its breach notification dated 23 May 2018[77] and in its compliance dated 02 February 2021.[78] Hence, both AIGSS and Medicard admitted that the PIC lost control and unauthorized persons acquired the personal data of the data subjects.

Further, the HR employee instructed the iHub Medicard Nurse, and not the Medicard Alabang Officer, to "encrypt and password protect each APE result before sending it individually" to the six (6)

---

[73] *Id.*
[74] *Id.* at 2-3.
[75] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).
[76] Full Report, 28 September 2018, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[77] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc., NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[78] Full Report, 02 February 2021, at 2-3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

employees.[79] The Medicard Alabang Officer, however, voluntarily undertook to send the APE results without following "the agreed process for handling APE results."[80]

Finally, AIGSS submitted a copy of the email from the employee who reported the breach.[81] The employee reported that their x-ray result file was incorrectly placed in another person's APE file, which shows that the recipients were able to open and view the contents of the APE results.[82]

The lack of security measures enabled the viewing of such personal information by the four (4) AIGSS employees, which should be sufficient to form a reasonable belief for the PIC.[83]

Nonetheless, the third requisite is not present due to the security measures that AIGSS implemented after the breach.

The Commission takes this opportunity to discuss the factors considered in determining the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

> Section 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.
>
> . . .
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give

---

[79] Full Report, 28 September 2018, at 1, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[80] *Id.* at 2.
[81] Compliance, 29 March 2021, Annex 3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[82] *Id.*
[83] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> rise to a real risk of serious harm to any affected data subject.[84]

For this purpose, the phrase "likely to give rise to a real risk" in Section 11 (C) means that a link exists between the breach and the possible resulting harm to any affected data subject.[85] The risk must be apparent and not the product of mere speculation.[86] Serious harm means that the consequences and effects to any affected data subject is significant based on the surrounding circumstances of the breach.[87]

In determining whether the unauthorized acquisition is likely to give rise to real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.

In this case, the unauthorized acquisition of information was due to the inadvertent transmittal of all the APE results to the four (4) AIGSS employees.[88] There is no showing that the AIGSS employees deliberately intended to obtain the information of other employees, as one of the four (4) recipient employees even reported the incident to the AIGSS Privacy Team.[89] The erroneous transmittal stemmed from the Medicard Alabang Officer's misunderstanding of the directive to send the results to the iHub Medicard Nurse,[90] as shown in the Medicard Alabang Officer's explanation in the breach's email thread.[91]

---

[84] NPC Circ. No. 16-03, § 11.
[85] NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8 (NPC 2023) (unreported).
[86] *Id.*
[87] *Id.*
[88] Full Report, 28 September 2018, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[89] Compliance, 29 March 2021, Annex 3, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[90] Full Report, 28 September 2018, at 1, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[91] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Thus, the objective of the unauthorized acquisition was not for fraudulent purposes.

It must be emphasized that the nature and amount of information involved in the breach—name, employee ID number, age, civil status, and medical information—are important details with respect to availing the medical benefits under Medicard's Corporate Health Program.[92]

Nonetheless, the security measures implemented by AIGSS prevented the occurrence of the risk of serious harm to the affected data subjects.

AIGSS notified the affected data subjects.[93] After one (1) of the recipient employees reported the incident on 10 March 2018,[94] AIGSS' Privacy Team initiated a review of the incident on the same date and implemented "remediation measures to contain the breach."[95] Thereafter, AIGSS reported that within seventy-two (72) hours it obtained email confirmation from the four (4) recipient employees that "the email had been deleted and was not retained or used by them."[96] Furthermore, AIGSS reported that it sent an email to all six (6) affected employees to notify them of the incident.[97] The notification states:

> Dear [],
>
> We very much regret to advise you that we recently became aware of an incident involving your sensitive personal data. In compliance with the Data Privacy Act (Republic Act 10173) and AIG Shared Services Data Privacy Reporting Procedure, we are informing you that your APE Results containing sensitive personal information were inadvertently sent by a Medicard employee to unauthorized recipients last March 9, 2018.

---

[92] Compliance, 29 March 2021, at 1-2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[93] *Id.* Annex 5-A to 5-D.
[94] Full Report, 28 September 2018, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[95] *Id.*
[96] *Id.* at 3.
[97] *Id.* at 5.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> You may get your own APE results in the attachment then delete all communications pertaining to the subject and its attachments. Please do not forward to any other users and refrain to reproduce it. Rest assured that we are coordinating and in communication with Medicard to ensure that all measures are being taken to protect your sensitive personal information and ensure that this will not happen again. A request has been sent to unauthorized recipients to delete all communications pertaining to the subject and its attachments. We will also request Medicard to do the same on the person who sent the email and a confirmation that it has been deleted.
>
> You can reach out to me or to BP Jr. our Data Protection Officer for AIG Shared Services – Business Processing Inc. (email address at [ ] with contact number [ ] ; cell number [ ]) for additional information regarding the breach, and for any support or clarification.
>
> Lastly, please send us a confirmation that you have deleted the said email.
>
> Thank you[.][98]

As proof of notification, AIGSS submitted an email notification regarding the breach (sent on 12 March and 13 March 2018), and confirmation of deletion from the four (4) recipients.[99]

Section 18 (C) of NPC Circular 16-03 provides the required content of proper notification of affected data subjects:

> Section 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. *Content of Notification*. The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;

[98] Compliance, 29 March 2021, Annex 5-A to 5-D, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[99] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

3. measures taken to address the breach;
4. measures taken to reduce the harm or negative consequences of the breach;
5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. any assistance to be provided to the affected data subjects.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.[100]

Further, Section 18 (D) of NPC Circular 16-03 provides the required form of proper notification:

> Section 18. *Notification of Data Subjects.* The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> D. *Form.* Notification of affected data subjects shall be done **individually, using secure means of communication, whether written or electronic.** The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and **to safeguard against further unnecessary disclosure of personal data.** The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: *Provided further*, that the personal information controller shall establish **means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.**[101]

[100] NPC Circ. No. 16-03, § 18 (C).
[101] *Id.* § 18 (D).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

The notification sent to affected data subjects must contain sufficient information on the nature of the breach incident, the personal data involved, the measures taken by the PIC to address the breach and to reduce harm or negative consequences of the breach, and the assistance it extended to its affected data subjects.[102] Further, the form of notification must be individual and must be made through secure means of communication, whether written or electronic.[103] The PIC must provide the data subject with the means to exercise their rights and obtain more detailed information relating to the breach.[104]

In this case, the Commission finds that the email notification complied with the requirements under Section 18 (C) and Section 18 (D) of NPC Circular 16-03.[105] The email notification contained information on the nature of the breach incident, the personal data involved, the measures taken by AIGSS to address the breach and to reduce harm or negative consequences of the breach, and a contact number that data subjects can use to obtain assistance and information.[106] Further, it was sent individually through email.[107] Thus, the notification enabled the affected data subjects to take measures to protect themselves from the consequences of the breach.

The Commission acknowledges the efforts of AIGSS to promptly notify the affected data subjects and implement security measures. In contrast, however, the Commission strongly reprimands Medicard for its failure to take action and its mere reliance on the measures taken by AIGSS.

The Commission agrees with AIGSS that Medicard is the PIC. As explained by AIGSS in its Compliance dated 29 March 2021:

> 5. The annual physical examinations of these 6 employees and any tests for the purposes of these examinations were carried out by Medicard at its Alabang clinic by Medicard's doctors, nurses, and staff based on their professional knowledge, skill, and expertise. AIGSS-MS and AIGSS-BPI naturally ha no input into

---

[102] NPC BN 18-198, 23 September 2021, at 4 (NPC 2021) (unreported).
[103] NPC Circ. No. 16-03, § 18 (D).
[104] *Id.*
[105] *Id.* § 18 (C) - (D).
[106] NPC BN 18-198, 23 September 2021, at 4 (NPC 2021) (unreported).
[107] NPC Circ. No. 16-03, § 18 (D).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> the conduct of such physical examinations. **The purposes for which Medicard collects, uses, discloses, and/or processes the personal information found in the results of APEs as well as the methods used by Medicard in collecting, using, disclosing, and processing the said personal information is entirely in the control of Medicard. Medicard provides the APE results directly to the employees and not to either AIGSS-BPI or AIGSS-MS.** In the circumstances, Medicard was the Personal Information Controller in respect of the personal information found in the APE results and was obliged to protect such personal information from, amongst other things, accidental disclosure.[108]

Clause 7 of the Agreement between AIGSS and Medicard[109] further confirms that Medicard is the PIC:

> [I]t is hereby agreed that it is the sole responsibility of the COMPANY to obtain from the MEMBERS the consent herein specified and that **MediCard shall have all the right to rely on the representation by the COMPANY that this consent shall have been duly and timely obtained.** The COMPANY shall hold MediCard free and harmless from and against any and all suits or claims, actions, or proceedings, damages, costs and expenses, including attorney's fees, which may be filed, charged or adjudged against MediCard or any of its directors, stockholders, officers, employees, agents, or representatives in connection with or arising from the **use by MediCard of the MEMBER'S medical records and other personal information pursuant to this Agreement and disclosure of such information to the COMPANY and its representatives pursuant to MediCard's reliance on the COMPANY'S representation and warranty that MediCard has the authority to examine, use or disclose, as the case may be, said medical records or personal information.**[110]

While there is shared responsibility between AIGSS and Medicard in that AIGSS was responsible for obtaining its employees' consent for processing of their information, ultimately it is still Medicard that processes their personal information to provide health insurance coverage. Moreover, it was Medicard's own personnel that

---

[108] Compliance, 29 March 2021, at 2, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021). Emphasis supplied.
[109] Full Report, 02 February 2021, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2021).
[110] *Id.* Emphasis supplied.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

inadvertently sent the APE results to the four (4) AIGSS employees, neglecting the protocol of encryption and password protection.[111]

There is no showing, however, in any of Medicard's submissions that it made efforts to notify its affected data subjects. It merely stated in its Full Report that it did not notify because it deemed the incident as "minimal/low risk."[112] It reasoned as follows:

> **We did not perform immediate breach notification because we considered the incident as low/minimal risk and would not cause harm to the 6 data subjects because the recipients of the APE Results were all within AIG.** MediCard is committed to complying with RA 10173. We would like to ensure that we are complying with the breach notification requirements even though AIG claimed that they have already reported the breach/incident to the Commission.
>
> MediCard was invited by Deputy Commissioner Ivy Patdu for a meeting last May 22, 2018 to discuss about Data Sharing Agreement and the AIG incident was brought up. We were advised by DepCom Patdu and Atty Mike to perform a breach notification and not to rely on AIG's notification to ensure that Medicard performed its duty as PIC.[113]

The Commission finds that Medicard's reasoning is not justified. If Medicard was truly committed to complying with its obligations under the DPA, as it claims, it should have promptly notified both the NPC and the affected data subjects upon receipt of AIGSS' email informing it of the incident as early as 13 March 2018.[114] Instead, Medicard sent a notification to the NPC only on 23 March 2018, fourteen (14) days after the breach.[115] Even worse, there is no showing that Medicard made any effort to notify the data subjects.

---

[111] Full Report, 28 September 2018, at 1, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018).
[112] Personal Data Breach Notification from Medicard Philippines, Inc., 23 May 2018, *in* In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation - Management Services (ROHQ), and Medicard Philippines, Inc. – Festival Alabang Clinic, NPC BN 18-033 and NPC BN 18-076 (NPC 2018). Emphasis supplied.
[113] *Id.* Emphasis supplied.
[114] *Id.*
[115] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

The Commission sternly reminds Medicard that although it was appropriate to implement security measures within its organization, such measures were prospective and insufficient to protect the affected data subjects from the risk they were already exposed to.[116] The purpose of notification is to provide data subjects with an opportunity to take the necessary precautions to protect their own data against the possible effects of the breach.[117] As such, PICs such as Medicard are required to "establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach."[118] Data subject notification is an essential obligation of a PIC,[119] and Medicard utterly failed to fulfill such obligation in this case.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-033 In re: AIG Shared Services – Business Processing Inc. and AIG Shared Services Corporation – Management Services (ROHQ) (AIGSS), and NPC BN 18-076 In re: Medicard Philippines, Inc. – Festival Alabang Clinic (Medicard) is **CLOSED.**

The Commission **DIRECTS** the Compliance and Monitoring Division (CMD) to conduct a Compliance Check on the sufficiency of Medicard's security measures involved in the processing of personal data.

SO ORDERED.

City of Pasay, Philippines.
02 August 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[116] Resolution, NPC BN 20-149 In re: National Privacy Commission 20 August 2020, at 6 (NPC 2020) *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Resolution-NPC-BN-20-149-In-re-NPC.pdf (last accessed 02 August 2023).
[117] NPC Circ. No. 16-03, § 18 (D).
[118] *Id.*
[119] Order, NPC BN 21-035, 01 June 2021, at 4 (NPC 2021) (unreported).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

(on official leave)
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

SG
Data Protection Officer
AIG Shared Services – Business Processing, Inc.
AIG Shared Services Corporation – Management Services (ROHQ)

RCM
Data Protection Officer
Medicard Philippines, Inc.

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

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228