IN RE: MYHEALTH CLINIC **NPC BN 18-143**

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a breach involving the unintentional disclosure of drug test results of employees from other companies to Ingram Micro Philippines, Inc. (Ingram).

Facts

MyHealth is engaged in the business of delivering ambulatory and outpatient health care services.[1] In July 2018, Dr. MIS, MyHealth's employee, sent a series of emails to Ingram, one of MyHealth's clients, with an attached file titled "Consolidated [Annual Physical Examination] Completion Tracker and Random Drug Test Results" (Reports).[2] Dr. MIS sent these emails as part of MyHealth and Ingram's contractual arrangement to advise Ingram of the status of the services availed by its employees.[3]

The Reports contained the names of the employee and employer, requested medical procedures, and drug test results.[4] The Reports, however, erroneously included random drug test results of twenty (20) individuals employed by MyHealth's other clients.[5]

On 01 August 2018, MyHealth through a Letter dated 31 July 2018 notified the National Privacy Commission (NPC) of the breach.[6] To

[1] Initial Breach Report, 31 July 2018, at 1, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2018).
[2] Full Breach Report, 14 August 2018, at 2, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2018).
[3] Initial Breach Report, 31 July 2018, at 1, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2018).
[4] *Id.*
[5] *Id.*
[6] *Id.*

address the breach, MyHealth stated that it immediately sent an email advisory to Ingram and requested that it disregard the reports.[7] MyHealth added that it implemented a "recall" process to retrieve the files from Ingram's mailbox and formally sent notification letters to the affected data subjects.[8] Finally, to prevent recurrence of the incident, MyHealth proposed to implement stricter policies and conduct data privacy reorientation seminars for all its personnel and staff handling personal information.[9]

On 09 August 2018, NPC, through its Complaints and Investigation Division (CID), directed MyHealth to submit a full report detailing the incident and to provide the information that was lacking from MyHealth's initial report.[10]

On 14 August 2018, MyHealth submitted its Full Report.[11]

On 10 May 2022, the CID directed MyHealth to submit its Post-Breach Report within 15 days from receipt thereof.[12] It directed MyHealth to submit (1) proof of measures undertaken to address the breach, (2) proof of its request to delete the information, (3) proof that Ingram agreed to such request, (4) proof of action undertaken against the erring personnel, and (5) proof of receipt of the notification sent to the affected data subject.[13]

On 09 June 2022, MyHealth submitted its Post-Breach Report.[14] In addition to its narration in the initial notification, MyHealth explained that it discovered the breach in an email thread dated 31 July 2018 where Dr. MIS wrote "please disregard the DT patients from other companies." The Post-Breach Report disclosed that Dr. MIS admitted that she failed to remove the drug test results of the other clients before sending the emails to Ingram.[15] Further, MyHealth clarified that "the incident arose purely out of human/mechanical error, sheer inadvertence and excusable oversight, and not due to MyHealth's

---

[7] Initial Breach Report, 31 July 2018, at 1, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2018).
[8] *Id.*
[9] *Id.*
[10] Email from the CID, 09 August 2018, at 1-2, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2018).
[11] Full Report, 14 August 2018, at 1-2, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2018).
[12] Order, 10 May 2022, at 2, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2022).
[13] *Id.* at 1-2.
[14] Post-Breach Report, 09 June 2022, at 2, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2022).
[15] *Id.*

system/procedures.[16] Additionally, MyHealth stated that Ingram responded and confirmed that it deleted the email containing the drug test results.[17]

MyHealth also stated that it imposed disciplinary action against Dr. MIS for her direct involvement in the breach.[18]

Finally, MyHealth submitted its new process flow for the release of results to prevent the recurrence of the breach. [19]

Issue

Whether MyHealth conducted proper breach management, including the implementation of reasonable and appropriate security measures.

Discussion

The Commission finds that MyHealth conducted proper breach management and implemented reasonable and appropriate security measures to address the incident. The Commission resolves to close the matter.

Section 20 (a) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) provides that a Personal Information Controller (PIC) should implement reasonable and appropriate security measures to protect personal information:

> Section 20. *Security of Personal Information.* (a) The **personal information controller must implement reasonable and appropriate 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.[20]

---

[16] *Id.*
[17] Post-Breach Report, 09 June 2022, at 2, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2022).
[18] *Id.* at 3.
[19] *Id.* Annex A.
[20] 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 § 17 (d) (3) (2012).

Further, Section 18 (C) of NPC Circular 16-03 (Personal Data Breach Management)[21] provides for the PIC's obligation to inform its data subjects of the measures it took to address the breach:

> 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;
> 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.[22]

A PIC, such as MyHealth, must notify its data subjects within seventy-two (72) hours upon knowledge of or reasonable belief that a personal data breach has occurred, in a manner that would allow the data subjects to protect themselves against the possible effects of the breach.[23]

In this case, MyHealth promptly and sufficiently notified the affected data subjects about the breach and detailed the security measures implemented to address it.[24]

In its notification to the affected data subjects, MyHealth provided a detailed explanation of how the breach occurred. To ensure that the data subjects were fully informed, MyHealth enumerated in its letter the specific information included in the drug test results that were inadvertently disclosed to Ingram.[25]

---

[21] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 17 (C) (15 December 2016).
[22] *Id.* § 18 (C).
[23] *Id.* § 18 (A).
[24] Post-Breach Report, 09 June 2022, Annex B, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2022).
[25] *Id.*

MyHealth stated that it has sent an email advisory requesting unintended recipients of Ingram who received several emails from MyHealth to delete the test results contained in those emails.[26] To recover the compromised personal data, MyHealth implemented a "recall" process to retrieve the test results from the mailbox of the unintended recipients.[27] MyHealth then assured its affected data subjects that it would implement stricter policies and conduct data privacy orientation seminars for its employees.[28]

Further, according to its Post-Breach Report, MyHealth revised its process flow for releasing results, designed to prevent future breaches.[29] It reported that in the updated process for releasing soft copies of medical records, the records must be scanned and saved as PDF files, with each filename reflecting the patient or employee's name.[30] Additionally, the PDF files must be encrypted for security.[31] MyHealth's releasing staff must log the recipient's email address in the logbook and verify that the attached files to be sent through email belong to the intended recipient.[32] The staff must also record the date and time of submission and request the recipient to acknowledge receipt of the records.[33]

Further, MyHealth carefully considered Dr. MIS's actions and subjected her to disciplinary actions.[34]

Lastly, MyHealth held data privacy reorientation seminars for all its personnel and staff handling personal information to address the incident and prevent its recurrence.[35]

Thus, the actions that MyHealth took to address and prevent the recurrence of the breach are sufficient to close the matter.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-143 In re: MyHealth Clinic is **CLOSED.**

---

[26] Initial Breach Report, 31 July 2018, at 1, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2018).
[27] *Id.*
[28] *Id.*
[29] Post-Breach Report, 09 June 2022, Annex B, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2022).
[30] *Id.* Annex A.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] Initial Breach Report, 31 July 2018, at 1, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2018).
[35] Post-Breach Report, 09 June 2022, at 3, *in* In re: MyHealth Clinic, NPC BN 18-143 (NPC 2022).

SO ORDERED.

City of Pasay, Philippines.
12 August 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

NIG
Data Privacy Officer

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