IN RE: ASIAN HOSPITAL AND MEDICAL CENTER **NPC BN 18-021**

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

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is a breach notification submitted by Asian Hospital and Medical Center (AHMC) involving the access of a patient's chart by third persons.

Facts

On 15 February 2018, the data subject was admitted as a patient at AHMC.[1] During the duration of her admission, AHMC's Guest Services Department received numerous inquiries about her.[2]

On 16 February 2018, a group of people, some introducing themselves as police and military personnel, came to the nurses' station asking for the patient's whereabouts.[3] The hospital's security team, assisted by the police, later escorted the group outside of the hospital to prevent any further commotion.[4]

On the same day, the Manager of the General Nursing Unit (GNU) informed AHMC's Data Protection Officer (DPO) of a possible data breach.[5] The GNU Manager narrated that he received an unverified report concerning a photo of AHMC's Hospital Information System (HIS) that shows the patient's name, age, date of birth, and medical diagnosis.[6] The DPO informed the GNU Manager that he will initiate

[1] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*

an investigation on the alleged breach in accordance with AHMC's Data Privacy Breach Protocol.[7]

AHMC's Medical Informatics Team (MID) initiated the extraction of the names of the personnel who viewed the patient's chart.[8] The MID submitted two reports, which are those who searched the patient's name (search log) and those who accessed the patient's chart (view log).[9]

On 17 February 2018, the patient was discharged from the HIS and was physically discharged from the hospital the following day.[10]

As part of the investigation, on 19 February 2018, the DPO conducted interviews with the GNU Manager and the Medical Information Services Manager.[11]

After the initial investigation, AHMC discovered that a photo of the patient's personal data was already posted in a Facebook group of what appears to be composed of the patient's creditors.[12] At this point, AHMC stated that it "has established reasonable belief and determination that a personal data breach indeed transpired."[13] As a result, AHMC conducted a full investigation on how an unauthorized person took a photo of its HIS.[14]

On 22 February 2018, AHMC notified the patient through mail sent to her home address.[15]

On 22 February 2018, AHMC notified the National Privacy Commission (NPC) of the breach.[16]

---

[7] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[14] *Id.*
[15] *Id.* at 4.
[16] *Id.* at 2.

On 06 October 2020, the NPC, through its Complaints and Investigation Division (CID) issued an Order requiring AHMC to submit its Full Breach Report within fifteen (15) days from receipt.[17]

On 19 October 2020, AHMC submitted its compliance,[18] together with the following documents: (1) a copy of its initial report;[19] (2) a summary of employees who underwent the internal investigation or "dialogue";[20] (3) its security incident report;[21] and (4) the remedial measures taken to address the incident and prevent its recurrence.[22]

In its compliance, it stated that it issued show cause memoranda and conducted a dialogue session with all personnel whose names were recorded in the search log and view log based on the report of the MID.[23] AHMC also reviewed the closed-circuit television (CCTV) camera footage.[24]

AHMC, through its investigation, determined that a member of the hospital staff took a photo of the patient's chart from AHMC's desktop using her mobile phone and forwarded the photo to a Facebook messenger group chat.[25]

As a result, AHMC imposed sanctions on all its personnel who violated the hospital's policy and procedure under the hospital's Code of Ethics.[26]

AHMC also stated that it took remedial measures to address the incident and prevent its recurrence and attached proof, including:

1. Strengthened and improved hospital policies and reiteration of protocols to all AHMC end users.
    i. Information security (PL-MID-004)

---

[17] Order, 06 October 2020, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[18] Response Letter dated 19 October 2020, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[19] Compliance, 19 October 2020, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[20] *Id.* Annex A.
[21] *Id.* Annex B.
[22] *Id.* Annex C.
[23] Response Letter dated 19 October 2020, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[24] *Id.*
[25] *Id.*
[26] *Id.*

ii. Access Matrix Security (PL-MID-002)

2. Reinforced Violations on Computer, Information Security & Data Privacy under the Hospital's Code of Ethics.
3. Integration of Data Privacy Act trainings for all newly hired employees under the "Safety Culture Program."
4. Confidentiality agreement[s] were ensued between AHMC and hospital staff, doctors, outsourced personnel and consultant and third party vendors.
5. Data Privacy Initiatives such as "Think Before You Click", as a social media reminder for all hospital employees, patients and visitors.
6. Integration of Data Privacy Act video materials in all AHMC's Devant LED Informercial platform.[27]

Issue

Whether AHMC conducted proper breach management, including the implementation of reasonable and appropriate security measures and notification of the affected data subject.

Discussion

The Commission finds that AHMC conducted proper breach management and implemented reasonable and appropriate security measures in addressing the breach. AHMC has also sufficiently notified the patient. Thus, 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 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.[28]

[27] *Id.*
[28] 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 § 20 (a) (2012).

Similarly, Section 17 (D) of NPC Circular 16-03 (Personal Data Breach Management) provides a PIC with the obligation to notify the NPC of a personal data breach.[29] The provision also outlines the content of notification specifically the measures that a PIC took to address the breach:

> Section 17. *Notification of the Commission*. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification*. The notification shall include, but not be limited to:
>
> . . .
>
> 3. Measures Taken to Address the Breach
>
> a. description of the measures taken or proposed to be taken to address the breach;
> b. actions being taken to secure or recover the personal data that were compromised;
> c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
> d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
> e. the measures being taken to prevent a recurrence of the incident.[30]

As early as its Initial Report, AHMC narrated the measures it took to address the breach following Section 20 (a) of the DPA and Section 17 (D) (3) of NPC Circular 16-03.

Upon receiving a report of a potential data breach, AHMC initiated its Data Privacy Breach Protocol.[31] This included the extraction of the names of the personnel who accessed the patient's chart on the HIS and the conduct of interviews and dialogues with the involved personnel.[32]

---

[29] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §17 (D)(3) (15 December 2016).
[30] *Id.*
[31] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[32] *Id.*

As part of its remedial measures, AHMC stated that it strengthened and improved the hospital's policies, specifically its Information Security Policy and Access Matrix Security Policy, and re-trained all its employees and medical staff on these policies. [33]

Further, AHMC reinforced its provisions on "Violations on Computer, Information Security, and Data Privacy" under the hospital's Code of Ethics.[34] This included the imposition of the penalty of dismissal on the first offense for the following violations:

> Computer, Information Security and Data Privacy[35]
>
> . . .

VIOLATIONS on Computer, Information Security and Data Privacy	**PENALTIES**			
	1st Offense	2nd Offense	3rd Offense	4th Offense
1. Willful non-observance of Computer Information Security and Data Privacy Policy, resulting in disruption of Hospital's operations, procedure, activities, and breach of information.	**Dismissal**			
2. Unauthorized Disclosure of Personal Information and Sensitive Personal Information of data subjects to co-employees, relatives, friends	**Dismissal**			

[33] Compliance, 19 October 2020, Annex C, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[34] *Id.*
[35] *Id.*

and the like that will lead to Personal Data Breach. **3. Concealment of knowledge on incidents of breach information.**	**Dismissal**			

In addition, AHMC integrated data privacy trainings for all newly hired employees in its Safety Culture Program which aims "to provide awareness and preventive action in response to possible hazard to individual and hospital-wide safety."[36]

AHMC also reiterated its confidentiality agreements between AHMC and its staff, doctors, outsourced personnel, consultants, and third-party vendors.[37] In its confidentiality agreements, AHMC explained that it has "a legal and ethical responsibility to safeguard the privacy of all patients and protect information that is identified as confidential."[38]

Further, AHMC submitted its Data Protection Vendor Consent Form, prepared by Metro Pacific Hospital Holdings, Inc. Hospital Group, which requires its suppliers to consent before AHMC processes personal data in relation to supplier registration and accreditation.[39]

Finally, AHMC created data privacy initiatives, such as "Think Before You Click," a reminder on using social media shared with all hospital employees, patients, and visitors.[40] It also included data privacy video materials on its LED informercial platform. [41]

It is the obligation of the PIC, such as AHMC, to ensure that it promptly and properly notifies its affected data subjects of the

---

[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Compliance, 19 October 2020, Annex C, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2020).
[40] *Id.*
[41] *Id.*

breach.[42] The Commission has consistently emphasized that the purpose of the notification to the data subjects is to allow them to take the necessary precautions or other measures to protect themselves against its possible effects.[43]

In this case, AHMC notified the patient through mail.[44] It submitted a copy of the letter and a 2GO Express receipt as proof of mailing to the patient's home address.[45]

In its letter, AHMC provided a narration of how the breach occurred, the personal data involved, and the results of its initial investigation.[46]

AHMC also enumerated the measures it undertook upon receiving information pertaining to the breach.[47] It also informed the patient that it will be issuing show cause memoranda to the responsible personnel and improve the security safeguards to its HIS. [48]

Further, AHMC provided the patient with the contact details of its DPO and Risk Management Manager in case she needed any assistance or further information in relation to the breach.[49]

Given the foregoing, the Commission finds that the measures undertaken by AHMC have sufficiently addressed the incident and prevented its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-021 In re: Asian Hospital and Medical Center is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.

---

[42] NPC Circ. No. 16-03, § 18 (A).
[43] *Id.*
[44] Initial Report, 22 February 2018, at 2, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[45] *Id.*
[46] Letter Re: Data Privacy Breach, 22 February 2018, at 1, *in* In re: Asian Hospital Medical Center, NPC BN 18-021 (NPC 2018).
[47] *Id.* at 2.
[48] *Id.* at 2-3.
[49] *Id.* at 2.

13 November 2023.

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:

JC
Assistant Manager, Data Privacy and Regulatory Compliance
Asian Hospital and Medical Center

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