IN RE: BAGUIO GENERAL HOSPITAL AND MEDICAL CENTER **NPC BN 18-014**

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

ORDER

Before the Commission is the Compliance of Baguio General Hospital and Medical Center (BGHMC) dated 20 January 2022 in accordance with the Order dated 04 January 2022.

On 09 February 2018, BGHMC reported a potential breach in its organization.[1] LuzonHealth conducted a Data Quality Check in the Family Planning Facility of BGHMC, to provide support to the Family Planning section's recording, reporting, and maintenance of records.[2] In the course of the Data Quality Check, LuzonHealth asked the billing section of BGHMC for an electronic copy of all patients who availed of the Philippine Health Insurance Corporation (PHIC) for the years 2015 to 2017.[3] LuzonHealth copied the personal and sensitive information from the Family Planning registry logbook from 2016 to January 2018.[4] The employees of BGHMC who permitted access to the records of the patients' pieces of information presumed that it was permitted and approved by the Medical Center Chief.[5]

Further, the BGHMC stated that Luzon Health promised to delete all the processed information.[6] However, the latter failed to destroy or delete the same in the presence of BGHMC.[7]

---

[1] Baguio General Hospital and Medical Center initial notification report dated 09 February 2018
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] Baguio General Hospital and Medical Center initial notification report dated 09 February 2018
[6] *Id.*
[7] *Id.*

On 13 February 2018, the Commission, through its Complaints and Investigation Division (CID) ordered BGHMC to submit a Full Report expounding the details of the incident.[8]

On 15 March 2018, BGHMC submitted its Full Report dated 07 March 2018.[9] BGHMC reiterated that during the technical assistance provided by LuzonHealth, it was observed that the information of the registered Family Planning acceptors was processed using the devices of LuzonHealth.[10] In line with this, the Data Protection Officer (DPO) of BGHMC was tasked to verify whether the said activity was valid and authorized, considering the purpose of collecting the data and encoding using LuzonHealth's devices.[11]

BGHMC stated that the laptop used by LuzonHealth in processing the data was already out of the facility, thus, making the incident a potential breach.[12]

The incident involves the personal data of all in-patients who are PHIC members which was stored on a flash drive belonging to a BGHMC employee.[13] Further, it consists of complete name, age, address, diagnosis, and PHIC claims of approximately one hundred twenty thousand five hundred eighty-seven (120,587) affected data subjects.[14] Moreover, BGHMC also stated that the family planning method or device being used, and birthdate are also possibly involved in the breach incident.[15]

As to the measures taken by BGHMC, it stated that it issued a Confidentiality Agreement for the personnel of LuzonHealth and asked the same for an incident report on the unauthorized access of personal data.[16] It also advised the LuzonHealth to delete all the data that were processed. [17]

---

[8] Order dated 3 February 2018, National Privacy Commission
[9] Baguio General Hospital and Medical Center Letter (Full Report) dated 07 March 2018
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Baguio General Hospital and Medical Center Letter (Full Report) dated 07 March 2018
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] Baguio General Hospital and Medical Center Letter (Full Report) dated 07 March 2018

Further, to prevent the recurrence of the incident, BGHMC stated the following measures that it will take, thus:

> 1. All requesting parties should prepare a formal communication to be approved by the MCC.
> 2. The approved communication shall be photocopied. The original copy shall be given to the data privacy officer.
> 3. The DPO shall record the request on the following entries: Name and Contact number of the requesting body, the type of data they request, purpose of the collection of data.
> 4. The DPO shall issue a Confidentiality Agreement or a Data Sharing agreement depending on the nature and purpose.
> 5. The DPO shall orient the requesting on the data privacy policies, process and practices that the institution being followed.
> 6. The DPO shall be informed, notify and witnessed on how the data will be deleted or destroy upon serving its purpose that shall be documented through the Registry of Requested Data.[18]

Moreover, BGHMC stated that it was not able to recover the personal data since the device used was already out of its facility and brought to LuzonHealth's office.[19]

BGHMC's involved employees were also asked to issue an explanation letter and were advised not to allow the disclosure of personal and sensitive information of data subjects without acquiring first the approval from the Medical Center Chief.[20] It was also recommended by BGHMC's DPO to impose sanctions on employees who will allow disclosure of any information without any written request with the approval of the Medical Center Chief.[21]

In notifying the affected data subjects, BGHMC stated that only those patients who disclosed their contact numbers could be informed of the incident.[22] Further, there could be a delay in data subject

[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] Baguio General Hospital and Medical Center Letter (Full Report) dated 07 March 2018
[22] *Id.*

notification since BGHMC needed to review all the data involved and verify whether the affected data subjects have contact numbers in their records.[23] On the other hand, BGHMC stated that sending through snail mail would be costly and it cannot determine the funding resources to do the same.[24]

Lastly, BGHMC stated that it is requesting a data subject notification exemption citing that personal information controllers (PIC) may request for an exemption or postponement of notification to the Commission when it is not reasonably possible to notify the data subjects within the prescribed period.[25]

On 22 June 2021, the CID issued an Order directing BGHMC to submit the Post-Breach Report on the lacking information from the initial notification report within fifteen (15) days from receipt, the report should include:

1. Copy of the Hospital's Confidentiality Agreement for Third Party Data Processors
2. Copy of LuzonHealth's letter of explanation to the hospital and certification that the processed information was deleted.
3. Proof of the remedial measures conducted by the Hospital to address the breach.
   - Results of your investigation. (Please provide a copy)
   - Copy of the letter/incident report for the unauthorized access of information
4. Proof/Efforts made to notify the affected data subjects.
   - Assistance offered to affected data subjects.
   - Proof that Data privacy Awareness was indeed conducted by the DPO.[26]

On 30 July 2021, BGHMC submitted its Compliance to the Order dated 22 June 2021.[27] It includes the copies of the confidentiality agreement signed by the personnel of LuzonHealth and the DPO of BGHMC.[28]

---

[23] *Id.*
[24] *Id.*
[25] Baguio General Hospital and Medical Center Letter (Full Report) dated 07 March 2018
[26]Order dated 22 June 2021, National Privacy Commission
[27] Baguio General Hospital and Medical Center Letter (Compliance) dated 30 July 2021
[28] *Id.*

A copy of LuzonHealth's letter of explanation was also submitted. In the letter, it stated that it aims to assist the Family Planning clinic of BGHMC to have accurate data to show that it performs well in implementing Family Planning.[29] LuzonHealth also stated that it unintentionally violated BGHMC's protocol for data gathering.[30] Lastly, LuzonHealth claimed that it already deleted the copied data in their flash drives and computers.[31]

As proof of the remedial measures conducted by BGHMC to address the breach, it submitted a copy of the letter of its DPO addressed to the Medical Center Chief, with a list of the suggested measures it will take with regard to the incident, thus:

> a. A letter of explanation why the need to copy, encode and saved personal data of patient by the LuzonHealth since it was not communicated to your office for the approval of collection of personal and sensitive information of our patients.
> b. A Confidentiality Agreement for Third Party Data Processor must be signed by all Data Collectors to emphasized the protection of the data privacy of our clients.
> c. Must specify in their letter the manner on how are they going to managed, store and destroy the information gathered
> d. Must ensure our institution that all electronic copies of the data being gathered, stored and saved in their devices must be deleted and that only statistical numerical data shall be used for health presentation with no evident of personal identifiers present that directly identify to any of our patients
> e. That this incident together with the above documents to be accomplished by the LuzonHealth shall be reported to the National Privacy Commission their information for a potential data privacy breach.[32]

Further, BGHMC also submitted a copy of its correspondence letters with the involved persons in the incident.[33] It includes the reporting of the breach to the Medical Center Chief by the personnel who

---

[29] *Id.*
[30] *Id.*
[31] Baguio General Hospital and Medical Center Letter (Compliance) dated 30 July 2021
[32] *Id.*
[33] *Id.*

allowed the disclosure of the data in the belief that there was permission from the former.[34]

BGHMC also stated that there is "no assistance offered to Data Subject due to unavailability of complete address and contact number".[35] Moreover, BGHMC submitted copies of the certification of some of its employees together with photos as proof of attending an orientation of the Data Privacy Act of 2012.[36] In addition, BGHMC attached in its submission the list of employees who were required to attend the orientation.[37]

On 04 January 2022, the CID issued an Order directing BGHMC to submit additional information and documents within ten (10) days from receipt.[38] BGHMC was directed to submit the date of the Confidentiality Agreements, Certification of deletion issued by RTI International, and the number of affected data subjects.[39] BGHMC was also directed to submit proof of notification sent to the data subjects with contact numbers and the efforts made to notify data subjects who do not have contact numbers.[40]

On 19 January 2022, BGHMC requested through email an extension of ten (10) days to comply with the Order dated 04 January 2022.[41]

On 19 January 2022, the CID issued a Resolution granting BHGMC's request for an extension of an additional ten (10) days to comply with the original deadline, or until 31 January 2022.[42]

On 20 January 2022, BGHMC submitted its Compliance to the Order dated 04 January 2022.[43] The copies of the Confidentiality Agreement between the personnel of LuzonHealth and BGHMC were

---

[34] *Id.*
[35] Baguio General Hospital and Medical Center Letter (Compliance) dated 30 July 2021
[36] *Id.*
[37] *Id.*
[38] Order dated 04 January 2022, National Privacy Commission
[39] *Id.*
[40] *Id.*
[41] Baguio General Hospital and Medical Center email (Request for Extension of time to submit) dated 19 January 2022
[42] Resolution dated 19 January 2022, National Privacy Commission
[43] Baguio General Hospital and Medical Center Letter (Compliance) dated 20 January 2022

submitted.[44] Moreover, BGHMC provided that the information involved were "Name of Patient, Age, Hospital and Account Number, Confinement Period, Philhealth Package, Ward, Philhealth Membership, Province, ICD-10 Code/RVS, Breakdown of the Hospital Bill, Physician's Name for private patients"[45]. Further, BGHMC stated that there were one hundred three thousand and one hundred thirty-five (103,135) affected data subjects as per their report/records from 2015-2017.[46]

Moreover, BGHMC reiterated in its Compliance its request for exemption of data subject notification since it cannot notify the affected data subjects stating that the complete address and/or contact number of the data subjects is not available.[47]

The Commission denies the request for exemption of data subject notification and further directs BGHMC to notify the affected data subjects, submit proof of such notification, and implement additional measures to correct the breach.

Section 18 (A) of NPC Circular No. 16-03 provides:

> **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:
>
> ***A. When should notification be done***. The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.
>
> The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions

[44] *Id.*
[45] Baguio General Hospital and Medical Center Letter (Compliance) dated 19 January 2022
[46] *Id.*
[47] *Id.*

> or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.[48]

In this case, BGHMC failed to notify the data subjects arguing that there were affected data subjects who did not have contact numbers or complete addresses.[49] The Commission finds the reason of BGHMC insufficient. Further, the Commission reminds the PICs of its obligation to notify the affected data subjects of breach incidents involving personal data as a general rule. Considering that the incident involves sensitive personal information, the data were acquired by an unauthorized person, and it is likely to give rise to a real risk of serious harm to the affected data subjects, thus, this case falls under the mandatory notification requirement.

Section 11 of NPC Circular No. 16-03 provides for the requisites of mandatory data subject notification, thus:

> 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:
>
> 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

[48] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18(A) (15 December 2016) (NPC Circular 16-03).
[49] Baguio General Hospital and Medical Center Letter (Compliance) dated 19 January 2022

> believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

It is well established that the matter requires mandatory data subject notification as contemplated in the above-stated provision. In this case, all the requisites for mandatory data subject notification are present such as the involvement of sensitive personal information, the data being unauthorized accessed by LuzonHealth's employee, and the unauthorized acquisition of the data will likely give rise to a real risk to the affected data subjects.

Further, Section 3 (l) of NPC Circular No. 16-03 provides:

> **SECTION 3.** ***Definition of Terms*****.** For the purpose of this Circular, the following terms are defined, as follows:
>
> l. "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;**
> 3. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns, and
> 4. Specifically established by an executive order or an act of Congress to be kept classified. (emphasis supplied)[50]

Here, the incident includes age, diagnosis, PHIC claims/information, family planning method or device being used, and birthdates of the affected data subjects which are considered sensitive personal information.

---

[50] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule 1, §3(L) (15 December 2016) (NPC Circular 16-03).

Further, the second element is also apparent in this case, considering that BGHMC admitted that LuzonHealth copied the personal and sensitive information from the Family Planning registry logbook which is a clear acquisition by an unauthorized person.[51]

The third element is also present since the unauthorized acquisition of information by LuzonHealth's employees is likely to give rise to a real risk of serious harm to the affected data subjects since the laptop used in copying the information of the affected data subjects was brought out of BGHMC's premises.[52] Thus, there is the possibility that the copied information by LuzonHealth's employees may be leaked or used which would lead to serious harm to the data subjects.

In addition, it must be noted that there are one hundred three thousand and one hundred thirty-five (103,135) affected data subjects, which BGHMC must take into consideration in determining whether to notify the affected data subjects. Section 13 (B) of NPC Circular No. 16-03 provides that when there is uncertainty as to the need for notification, it must be taken into consideration the number of data subjects such as when there are at least one hundred (100) individuals involved.[53]

BGHMC's requested for exemption of data subject notification since the complete address and/or contact number of the affected data subjects are not available. However, BGHMC failed to justify that notification of data subjects would not be in the public interest or in the interest of the affected data subjects as provided in Section 18(B) of NPC Circular No. 16-03. There is nothing in BGHMC's submission that would satisfy and warrant granting its request for exemption of data subject notification. Thus, the Commission denies its request for data subject notification exemption considering that its justification does not fall under the conditions in granting such request.

---

[51] Baguio General Hospital and Medical Center initial notification report dated 09 February 2018
[52] *Id.*
[53] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, §13 (B) (15 December 2016) (NPC Circular 16-03).

Section 18 (B) of NPC Circular No. 16-03 provides for the conditions when the Commission may allow Personal Information Controllers (PIC) to be exempted from data subject 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:
>
> B. Exemption or Postponement of Notification.
> If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification.
> **A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.**
> The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach. (emphasis supplied)[54]

Additionally, Section 19 of NPC Circular No. 16-03, further provides additional factors in case of doubt in determining when the Commission may allow PICs to be exempted for data subject notification, thus:

> **SECTION 19.** ***Exemption from Notification Requirements***.
> The following additional factors shall be considered in determining whether the Commission may exempt a personal information controller from notification:
> A. Security measures that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, including measures that would prevent use of the personal data by any person not authorized to access it;
> B. Subsequent measures that have been taken by the personal information controller or personal information processor to

[54] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, §18 (B) (15 December 2016) (NPC Circular 16-03).

> ensure that the risk of harm or negative consequence to the data subjects will not materialize;
>
> C. Age or legal capacity of affected data subjects: *Provided*, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives.
>
> In evaluating if notification is unwarranted, the Commission may take into account the compliance by the personal information controller with the law and existence of good faith in the acquisition of personal data.[55]

In this case, BGHMC has not provided concrete evidence of the security measures implemented during and after the breach to mitigate the risk of harm to affected data subjects. Based on its submissions, BGHMC only conducted a data privacy seminar and submitted signed copies of the confidentiality agreements as its measures to address the breach.[56]

Furthermore, the Commission emphasizes that sensitive personal information such as patient records could expose individuals to real and significant risks like identity fraud when such was processed and acquired by unauthorized individuals.

Time and again, the Commission reminds the PICs to comply with its issuances and to take proactive steps in ensuring the safeguard of the personal data entrusted by data subjects to the PICs. Moreover, PICs must establish all reasonable mechanisms to ensure that all affected data subjects are made aware through proper notification of the breach incident.

Given the foregoing, BGHMC is directed to notify the affected data subjects and submit proof of such notification directly to the Commission's Compliance and Monitoring Division. The Commission stresses that data subject notification is the general rule. It is the PIC's obligation to notify the affected data subjects when a breach falls under mandatory data subject notification. Such

---

[55] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, §19 (15 December 2016) (NPC Circular 16-03).

notification is to allow the affected data subjects to take the necessary precautions to protect themselves against the possible effects of the breach.

In addition, to prevent similar instances from happening in the future, BGHMC is directed to implement additional measures to address the breach.

WHEREFORE, premises considered, the Commission **DENIES** Baguio General Hospital and Medical Center's request for exemption of data subject notification. Moreover, Baguio General Hospital and Medical Center is hereby **ORDERED** to **NOTIFY** the affected data subjects and **SUBMIT** proof of notification directly to the Compliance and Monitoring Division and to **IMPLEMENT** additional remedial measures to correct the breach from receipt of this Order within fifteen (15) days from receipt of this Order.

Further, the Commission **DIRECTS** the Compliance and Monitoring Division to issue appropriate orders necessary to evaluate and monitor the completeness of the Baguio General Hospital and Medical Center data breach notification and assess its breach management pursuant to NPC Circular No. 16-03 (Personal Data Breach Management).

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

ACB
Data Protection Officer
BAGUIO GENERAL HOSPITAL AND MEDICAL CENTER

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