Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap 486)

Accidental Disposal of Medical Records of Patients by Town Health Medical & Dental Services Limited

Report Number：R22 - 12326

Date Issued: 13 June 2022

Investigation Report
Accidental Disposal of Medical Records of Patients by
Town Health Medical & Dental Services Limited

Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) provides that "*the Privacy Commissioner for Personal Data may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report -*

(a) setting out -

(i) the result of the investigation;

(ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(iii) such other comments arising from the investigation as he thinks fit to make; and

(b) in such manner as he thinks fit."

This investigation report is hereby published in discharge of the powers under section 48(2) of the Ordinance.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
13 June 2022

Table of Contents

Investigation Report

Published under Section 48(2)
of the Personal Data (Privacy) Ordinance (Cap 486)

Accidental Disposal of Medical Records of Patients by Town Health Medical & Dental Services Limited

Executive Summary

Background

1. On 2 June 2021, the Office of the Privacy Commissioner for Personal Data (PCPD) received a data breach notification (Notification) from Town Health Medical & Dental Services Limited (Town Health). Town Health reported that one of its medical centres located in Fortress Hill (Medical Centre) had accidentally disposed of a carton box (Carton Box) containing patients' medical records. According to Town Health, its cleaning staff (Cleaner) mistakenly treated the Carton Box as waste and disposed of it on 14 March 2021 (Incident).

2. The Incident affected a total of 294 patients of the Medical Centre, which resulted in the loss of personal data including their names, telephone numbers, Hong Kong Identity Card numbers, addresses, dates of birth, diagnosis records, medication records and laboratory results, etc.

3. On receipt of the Notification, the PCPD immediately commenced a compliance check against Town Health to ascertain the relevant facts relating to the Incident. Upon receiving further information from Town

Health, the Privacy Commissioner for Personal Data (Commissioner) believed that Town Health's acts or practices in the Incident might have contravened the requirements of the Personal Data (Privacy) Ordinance (Ordinance), Chapter 486, Laws of Hong Kong. In July 2021, the Commissioner commenced an investigation in relation to the Incident against Town Health pursuant to section 38(b)(ii) of the Ordinance.

Investigation

4. During the course of the investigation, the Commissioner reviewed and considered the information provided by Town Health through six rounds of enquiries, including its procedures in handling medical records and the security measures adopted in safeguarding the medical records. To better understand the setting of the Medical Centre and the security measures adopted in processing and storage of the medical records, the Commissioner sent officers to conduct an on-site inspection. The Commissioner also considered the follow-up and remedial actions taken by Town Health in the wake of the Incident.

Findings and Contravention

Data Breach Incident

5. During the course of the investigation, the Commissioner came to the conclusion that the Incident was a data breach in which the Medical Centre of Town Health accidentally disposed of a carton box containing personal data of 294 patients.

6. Given that Town Health had control of the collection, holding, processing or use of the personal data concerned in the Incident, Town Health was deemed to be a data user under the Ordinance, and was required to comply

with the requirements of the Ordinance, including the six Data Protection Principles (DPP) set out in Schedule 1 to the Ordinance.

Serious Deficiencies in Data Security

7. Pursuant to DPP4(1), a data user is obliged to take all practicable steps to ensure that the personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use.

8. Having considered the evidence obtained during the course of the investigation, the Commissioner found that Town Health had serious deficiencies in terms of staff awareness of data protection, policy and staff training, which contributed to the accidental yet avoidable disposal of the Carton Box. The main reasons are summarised as follows:

(1) **Lack of staff awareness of data protection**: the Incident was mainly caused by human negligence. For the sake of work convenience, the health care assistant concerned at Town Health failed to take heed of data security. She neither placed the Carton Box properly nor affixed any labels to the Carton Box to indicate the contents therein and their purposes. Worse still, she placed the Carton Box near a trash bin that totally ignored the importance of the personal data placed therein. Such act was obviously negligent. Meanwhile, the Cleaner treated the Carton Box as waste for disposal only because the Carton Box was placed near the trash bin.

(2) Lack of effective policies and procedures: the policies and guidelines devised by Town Health on the protection of medical records were neither comprehensive nor specific. Even though the guidelines had been duly communicated to frontline staff of the Medical Centre, they failed to prevent the Incident from happening.

(3) **Lack of staff training:** Town Health did not provide training for its frontline staff regarding the protection of personal data, which was another critical factor contributing to their lack of awareness of data protection.

Data Retention

9. The Carton Box was about to be transferred to the central warehouse of Town Health for storage. The records contained therein belonged to 292 patients who had not visited the Medical Centre for more than seven years and two other patients who had their last visit in 2019.

10. Given that patients might seek medical treatment again or request for their medical records, the Commissioner considered it would generally be necessary for medical institutions to keep medical records for a longer period of time. Overall, the Commissioner considered that there was no information suggesting Town Health had kept the medical records concerned for a prolonged period of time. Town Health did not contravene the requirements of DPP2(2) in Schedule 1 to the Ordinance as regards the retention of personal data.

Data Breach Notification

11. Whilst there is no statutory requirement under the Ordinance prescribing a data user to notify the Commissioner and the data subjects for data breach incidents, or the period within which such notifications are required to be made, the Commissioner considered that owing to the sensitive nature of the personal data involved in the Incident, Town Health should have lodged the Notification earlier. **The Commissioner regretted to note that Town Health only lodged the Notification nearly three months after the Incident.**

Town Health contravened DPP4(1)

12. The Commissioner considered that since medical records were sensitive personal data, Town Health, being a data user managing hundreds of medical centres and possessing a large number of medical records of citizens, should devise comprehensive policies as to the collection, holding, processing and use of the medical records, conduct appropriate risk assessments, provide adequate training for its staff to instil data protection awareness, and take all practicable security measures in accordance with DPP4(1) to prevent any personal data held by it from unauthorised or accidental access, processing, erasure, loss or use.

13. The Incident revealed that Town Health: -

(1) Failed to examine and assess the risk of human negligence, thereby resulting in the failure to take appropriate measures to address the risk arising from the lack of awareness of employees on data protection;

(2) Failed to devise clear and adequate data security policies and guidelines to protect sensitive personal data; and

(3) Failed to provide adequate training for all relevant parties on the proper handling of personal data.

14. **In the present case, the Commissioner found that Town Health had serious deficiencies in ensuring the security of personal data. The Commissioner considered that Town Health had not taken all practicable steps to ensure that the medical records in question be protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP4(1) concerning the security of personal data.**

Enforcement Action

15. The Commissioner issued an Enforcement Notice to Town Health directing it to take the following steps to remedy the situation and prevent recurrence of the contravention:

(1) Conduct a comprehensive review and update on all its written policies and standard operating procedures/guidelines in relation to data protection, so as to provide medical centres with specific policies and operating procedures/guidelines;

(2) Devise effective measures to ensure staff compliance with the revised written policies and standard operating procedures/guidelines on data protection;

(3) Devise effective measures to monitor the compliance of staff or any third party responsible for cleaning services of medical centres with the requirements of the "*Cleaning Guidelines*";

(4) Provide training for staff members on data protection, record the training processes properly, and evaluate the level of participation of staff and effectiveness of the training; and

(5) Provide documentary proof to the Commissioner within two months from the date of the Enforcement Notice, showing the completion of items (1) – (4) above.

Recommendations

Medical records are sensitive personal data and should be treated seriously

16. Regardless whether personal data is lost by accident, leakage or improper disposal, the potential harm to individuals should not be underestimated, in particular when sensitive medical records are involved. Medical record is an important asset of the healthcare industry as it contains sensitive health and medical information of an individual. It is therefore crucial for medical service providers to ensure that medical records are properly managed and handled throughout their lifecycle. This is not only to comply with the provisions of the Ordinance, but also to shoulder moral responsibility for patients.

17. **The Commissioner recommends that organisations should establish and maintain a proper system for the responsible use and retention of personal data. A Personal Data Privacy Management Programme could assist organisations to effectively manage the lifecycle of personal data from collection to erasure, to handle data breach incidents promptly, and to ensure due compliance with the Ordinance. Meanwhile, organisations should appoint Data Protection Officer(s) to monitor compliance with the Ordinance and report any issues to the senior management.**

18. In addition to establishing effective policies and practices on data protection, data users should take steps to constantly monitor whether the policies and practices are duly observed by their employees, and provide them with comprehensive training in order to minimise human error. **The Commissioner recommends that organisations should holistically enhance employees' awareness of personal data protection and cultivate a personal data protection culture across the board. Organisations should provide employees with comprehensive training**

to incorporate personal data protection into their daily duties, with a view to reducing human error caused by a lack of awareness.

19. While data breaches in the online world are becoming pervasive in the era of digital age, data breaches cannot be overlooked in the "offline" world. Town Health and all data users processing personal data in physical form should not only learn a lesson from the Incident, but also nip similar incidents in the bud. **The Commissioner recommends that organisations should adopt the same level of security measures for the relevant systems in processing personal data, whether they are computerised or in physical form. While adopting reliable systems and security settings to protect systems from cyberattacks, organisations should also allocate resources to strengthen security measures in protecting physical data.**

While lodging data breach notification is not punitive, data users should not evade their obligations under the Ordinance

20. The Commissioner noted that many data users were overwhelmed by an incident of data breach. There is currently no statutory requirement under the Ordinance prescribing a data user to notify the Commissioner and the data subjects for data breach incidents, or the period within which such notifications are required to be made. In fact, when the PCPD receives data breach notifications, we will provide data users with appropriate advice to help them respond to data breach incidents promptly and take appropriate measures and actions in a timely manner, with a view to minimising the loss and damage done to organisations and data subjects. The PCPD will also provide advice to assist data users in improving their systems and policies for handling personal data to prevent the recurrence of similar incidents. On the contrary, any delay in action or in notifying the Commissioner of a data breach may result in multiplied or irreversible damage to organisations and data subjects, including both emotional and

actual financial harm. **The Commissioner recommends that when data users suspect or note the occurrence of a data breach incident, they should notify the PCPD as soon as possible. The PCPD will provide assistance and advice to help minimise the damage caused by the data breach incident and improve the personal data system.**

I. Introduction

1. On 2 June 2021, the Office of the Privacy Commissioner for Personal Data (PCPD) received a data breach notification (Notification) from Town Health Medical & Dental Services Limited (Town Health). Town Health reported that one of its medical centres located in Fortress Hill (Medical Centre) had accidentally disposed of a carton box (Carton Box) containing patients' medical records. According to Town Health, its cleaning staff (Cleaner) mistakenly treated the Carton Box as waste and disposed of it on 14 March 2021 (Incident).

2. The Incident affected a total of 294 patients of the Medical Centre, which resulted in the loss of personal data including their names, telephone numbers, Hong Kong Identity Card numbers, addresses, dates of birth, diagnosis records, medication records and laboratory results, etc.

3. On receipt of the Notification, the PCPD immediately commenced a compliance check against Town Health to ascertain the relevant facts relating to the Incident. Upon receiving further information from Town Health, the Privacy Commissioner for Personal Data (Commissioner) believed that Town Health's acts or practices in the Incident might have contravened the requirements of the Personal Data (Privacy) Ordinance (Ordinance), Chapter 486, Laws of Hong Kong. On 30 July 2021, the Commissioner commenced an investigation in relation to the Incident against Town Health pursuant to section 38(b)(ii) of the Ordinance.

II. Statutory Powers and Relevant Legal Requirements

Statutory Powers

4. The powers of the Commissioner are conferred by the Ordinance. According to section 8(1) of the Ordinance, the Commissioner shall monitor and supervise compliance with the provisions of the Ordinance, and promote awareness and understanding of, and compliance with, the provisions of the Ordinance.

5. Section 38 of the Ordinance empowers the Commissioner to conduct investigations under the following circumstances:

   (i) Where the Commissioner receives a complaint from the affected data subject or his representative, the Commissioner shall, in accordance with section 38(a)(i) and subject to section 39, carry out an investigation in relation to the relevant data user to ascertain whether the act or practice specified in the complaint is a contravention of a requirement under the Ordinance; or

   (ii) Where the Commissioner has reasonable grounds to believe that an act or practice relates to personal data has been done or is being done by a data user, which may be a contravention of a requirement under the Ordinance, the Commissioner may, in accordance with section 38(b)(ii), carry out an investigation in relation to the relevant data user to ascertain whether the act or practice is a contravention of a requirement under the Ordinance.

6. After initiating an investigation, the Commissioner may, in accordance with section 43(1)(a) of the Ordinance, for the purposes of the investigation be furnished with any information, document or thing, from such persons, and make such inquiries, as she thinks fit.

7. Section 48(2)(a) of the Ordinance stipulates that the Commissioner may, after completing an investigation and if she is of the opinion that it is in the public interest to do so, publish a report setting out the result of the investigation, and any recommendations or other comments arising from the investigation as the Commissioner thinks fit to make.

8. Section 50(1) of the Ordinance provides that in consequence of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, the Commissioner may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent recurrence of the contravention.

9. Under section 50A of the Ordinance, a contravention of an enforcement notice constitutes an offence which may result in a maximum fine at level 5 (i.e. HK$50,000) and imprisonment for 2 years on a first conviction.

Relevant Legal Requirements

Data User

10. The Ordinance, including the Data Protection Principles (DPPs) in Schedule 1 thereof, aims to regulate the acts and practices of a data user. Under section 2(1) of the Ordinance, a data user, in relation to personal data, means "*a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data*".

Personal Data

11. Data users falling within the purview of the Ordinance are required to comply with the DPPs in handling "personal data". Under section 2(1) of

the Ordinance, "personal data" means "*any data –*

(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the data is practicable."

Data Retention

12. DPP2(2) provides for the principle on data retention, which states that: -

"*All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used*".

Data Security

13. DPP4(1) provides for the principle on data security, which states that: -

"*All practicable steps shall be taken to ensure that any personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to –*
(a) the kind of data and harm that could result if any of those things should occur;
(b) the physical location where the data is stored;
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
(e) any measures taken for ensuring the secure transmission of the data".

14. "*Practicable*" is defined in section 2(1) of the Ordinance to mean "*reasonably practicable*".

15. Regarding the "harm" test set out in DPP4(1)(a) above, considerations have to be given on whether the security measures undertaken by the data users are commensurate with the sensitivity of the personal data concerned; and the harm that might result from unauthorised or accidental access to such data.

Data Breach Incident

16. The Ordinance does not define a data breach. A data breach generally refers to a suspected or actual breach of the data security of the personal data held by a data user that exposed the data to the risk of unauthorised or accidental access, processing, erasure, loss or use; unauthorised access or inspect and transfer, inappropriate disposal or management of documents containing personal data, etc.

Data Breach Notification

17. Currently, it is not a mandatory requirement under the Ordinance for a data user to notify the Commissioner or the relevant data subjects of a data breach. The Commissioner nevertheless has issued a revised "*Guidance on Data Breach Handling and the Giving of Breach Notifications*" [1] recommending the steps to be followed by data users in the event of a data breach incident.

[1] https://www.pcpd.org.hk//english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

III. Information and Evidence obtained from the Investigation

18. During the course of the investigation, the Commissioner reviewed and considered the information provided by Town Health through six rounds of enquiries, including its procedures in handling medical records and the security measures adopted in safeguarding the medical records. To better understand the setting of the Medical Centre and the security measures adopted in processing and storage of the medical records, the Commissioner sent officers to conduct an on-site inspection. The Commissioner also considered the follow-up and remedial actions taken by Town Health in the wake of the Incident.

Company Background

19. Town Health operates over 100 medical centres in Hong Kong, including centres for general practice, specialist consultation, and dental services. Town Health is a wholly owned subsidiary of Town Health International Medical Group Limited.

20. The address of the Medical Centre is Shop D2, G/F, Merlin Garden, 160 Electric Road, Fortress Hill, Hong Kong.

Shop front of the Medical Centre

Affected Personal Data

21. According to Town Health, the Carton Box contained medical records of 294 patients. Amongst them, 292 patients had not visited the Medical Centre for more than seven years whilst the remaining two visited the Medical Centre for the last time in 2019. The medical records in the Carton Box contained the following personal data of the relevant patients: -

(i) Names

(ii) Telephone numbers

(iii) Hong Kong Identity Card numbers

(iv) Addresses

(v) Dates of birth

(vi) Patient numbers

(vii) Medical card numbers

(viii) Diagnosis records

(ix) Medication records

(x) Laboratory results

Policies of Town Health on Data Security

22. During the course of the investigation, Town Health submitted its policies and guidelines relating to the protection of medical records as follows: -

23. Town Health submitted to the PCPD a set of untitled guidelines issued to its frontline staff in relation to the handling of personal data. Among others, there were five requirements on the proper handling of personal data of customers and three requirements on the handling of data breach incidents. In particular, the guidelines stated that "*before leaving the workstation, you should ensure that any customer information has been properly stored (e.g. patients' data needs to be reversed or covered) in order to prevent the information from being accessed by third parties or outsiders easily.*"[2]

24. Town Health submitted another set of untitled guidelines to the PCPD, which had been provided for its staff in relation to the handling, use and storage of medical records. This set of guidelines set out the proper practices on the handling, use and storage of medical records. However, the guidelines were silent on the requirements and procedures for the handling of "Inactive Medical Records".

The "*Cleaning Guidelines*"

25. Town Health stated that the staff of all medical centres were required to observe the requirements of the "*Cleaning Guidelines*" when disposing of

[2] Translation from the original Chinese text.

waste. The "*Cleaning Guidelines*" would also be provided to all cleaning staff when they were employed. The Commissioner specifically noted the following two requirements stated in the "*Cleaning Guidelines*":

(i) *Cleaning staff are not allowed to take away or discard any documents and "all items" of the clinic without authorisation, except for the rubbish in the trash bins.*

(ii) *Without the authorisation of the person in charge, "all items" in the clinic cabinet, shelf, table and doctor's room should not be taken away or discarded. "All items" include: all medicines, medical items, medical appliances, medical utensils, patients' records, forms filled with personal data, patients' medical reports and X-ray films, all computer software, hardware, etc...*[3]

26. Town Health stated that all the three aforementioned guidelines had been posted on the wall or cabinets of its medical centres before the Incident. The Quality Assurance Department and the regional officer-in-charge of Town Health were responsible in ensuring staff compliance with these guidelines.

Responses from Town Health to the Incident

27. Town Health stated that it was their long-standing practice to store medical records of patients, who visited the medical centres (including the Medical Centre) in the past three years, in document cabinets of the respective medical centres. This was to facilitate the use of such records when those patients seek medical consultation. At the same time, medical centres would classify the medical records of patients who had not visited the relevant medical centres for more than three years as "Inactive Medical

[3] Translation from the original Chinese text.

Records". The "Inactive Medical Records" would then be transferred to a central warehouse of Town Health for storage on a regular basis.

28. In the case of the Medical Centre, medical records of patients were kept on the document shelves behind the registration desk, and were only accessible to staff members or authorised personnel.

29. On 14 March 2021, a Health Care Assistant (HCA) of the Medical Centre inspected the medical records on the document shelves so as to filter out "Inactive Medical Records". During the process, she put the "Inactive Medical Records" into the Carton Box and intended to have the same transferred to the central warehouse of Town Health for storage. Since the HCA did not complete the inspection process at the material time and planned to continue the work on the following day, she placed the Carton Box temporarily on the floor within her working area (i.e. near a trash bin behind the registration desk). The Cleaner, who was responsible for the cleaning of the Medical Centre, mistakenly treated the Carton Box as waste and transported it away from the Medical Centre for disposal at noon of the same day.

30. On the morning of 15 March 2021, the HCA informed her supervisor of the Incident as soon as she found the Carton Box missing.

31. On 2 June 2021, Town Health lodged the Notification to the PCPD, stating that its cleaning staff who mistakenly treated a carton box containing medical records of patients as waste disposed of it on 14 March 2021.

Other Evidence and Facts of the Incident

32. According to Town Health, the Cleaner explained that since there was no label on the Carton Box and that the Carton Box was placed near the trash bin, he mistakenly treated it as waste and disposed of it.

33. Town Health submitted a CCTV footage capturing the Incident to the Commissioner, showing that the Cleaner was moving the Carton Box towards the entrance/exit of the Medical Centre. As seen from the footage, the Carton Box was a normal hard carton with an estimated size of 40 x 30 x 20 cm^3, and it was left open.

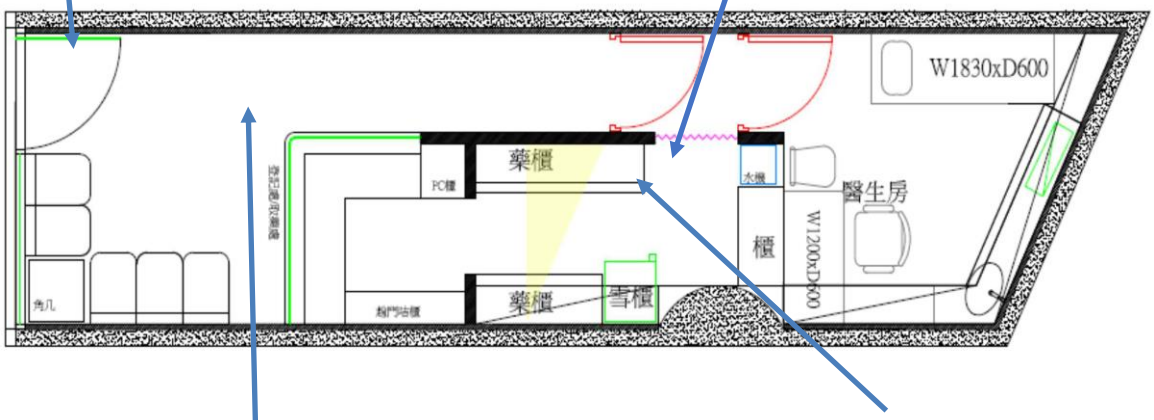
34. Town Health believed that the Carton Box was disposed of together with other general waste at the refuse collection point at Oil Street, North Point (about 200 metres away from the Medical Centre).

35. According to the information provided by Town Health and the on-site inspection of the Medical Centre by the officers of the PCPD, the Medical Centre could be divided into three main areas: (i) the patient waiting area; (ii) the working area of HCAs (mainly the space behind the registration desk); and (iii) the doctor's consultation room. It was noted that the Carton Box was placed on the floor near the trash bin within the working area of HCAs at the time when the same was removed by the Cleaner.

36. The diagram and photos below illustrate the layout of the Medical Centre. The location of the Carton Box and the trash bin at the time of the Incident were indicated therein:

Working area of HCAs[4]

Entrance of the Medical Centre



The HCA placed the Carton Box near a trash bin

The Cleaner moved the Carton Box towards the entrance/exit of the Medical Centre

The Carton Box contained medical records of 294 patients, which was mistakenly treated as waste and disposed of.

[4] The location of the trash bin shown in the picture was different from the one placed at the time of the Incident.

37. Town Health admitted that the HCA placed the Carton Box at an inappropriate location at the material time. Besides, Town Health submitted that the Medical Centre had undergone renovation works between 12 and 13 March 2021, including minor ceiling works, lighting works and refurbishment of the doctor's consultation room. During the on-site inspection conducted by the PCPD's officers, representatives of Town Health expressed that the Cleaner might have wrongly believed that the Carton Box contained debris from the renovation works and therefore disposed of it.

38. Town Health admitted that it had not provided any training on personal data protection for its frontline staff members prior to the Incident.

39. In addition to the 292 "Inactive Medical Records", the Carton Box also contained two medical records of recent years. Town Health speculated that the two medical records were temporarily put inside the Carton Box by the HCA after she had removed them from the document shelves for review. They were left inside the Carton Box at the material time because the reviewing process had not yet been completed.

Follow-up Actions and Remedial Measures

40. Town Health stated that upon discovery of the Incident, it immediately requested officers to proceed to the said refuse collection point and a recycling company nearby to locate the Carton Box but in vain.

41. Town Health stated that they had notified the two affected patients (who last visited the Medical Centre in 2019) of the Incident by phone. The other affected patients were informed of the Incident in writing.

42. Town Health dismissed the Cleaner and engaged a cleaning company to provide cleaning services for all medical centres of Town Health.

43. Town Health revised its "*Cleaning Guidelines*" in May 2021 and added the following requirements:

(i) All rubbish and items to be disposed of must be placed in the trash bins;

(ii) For rubbish unable to be put into trash bins, please put it in a garbage bag or carton box, and affix a label of "rubbish" to the outside and place it at a designated area. Cleaning staff should also be notified in advance if the same is to be disposed of; and

(iii) Cleaning staff may not discard any items printed with personal data in medical centres.[5]

44. Town Health provided the revised "*Cleaning Guidelines*" to the outsourced cleaning company, and instructed them to ensure that its staff adhere to the guidelines when performing their duties. In addition, each medical centre is required to assign an HCA to conduct evaluation on the performance of the cleaning company on a quarterly basis, including whether the "*Cleaning Guidelines*" are followed.

45. Town Health has also revised the standard operating procedures for the handling and proper storage of "Inactive Medical Records". The updated guidelines clearly stated that any storage box with "Inactive Medical Records" must be labelled for indication of content. The storage box containing medical records must not be left on the floor unattended. Staff members should place the storage box at a designated location before getting off work.

[5] Translation from the original Chinese text.

Responses from Town Health for the Delay of Submitting the Notification

46. During the course of the investigation, the Commissioner sought an explanation from Town Health as to the reasons for taking almost three months after the Incident (i.e. until June 2021) to submit the Notification to the PCPD. Town Health responded that its internal investigation commenced immediately after the Incident and continued in April 2021. Unfortunately, as the full records of the Incident were not properly maintained, coupled with the fact that the staff responsible for investigating and handling the Incident (including a General Manager) had resigned, Town Health could not determine the causes of the delay.

IV. Findings and Contravention

47. In accordance with DPP4(1), a data user is obliged to take all practicable steps to ensure that the personal data it holds should be protected against unauthorised or accidental access, processing, erasure, loss or use. In the present case, the factors considered by the Commissioner include: (i) whether the Incident is a data breach; (ii) who is the data user accountable for the data breach; and (iii) whether practicable steps have been taken by the data user to protect the personal data held by it in accordance with the requirements of DPP4(1).

48. In accordance with DPP2(2), a data user is obliged to take all practicable steps to ensure that personal data should not be kept longer than is necessary for the fulfillment of the purpose for which the data is or is to be used. In the present case, the Commissioner has also considered the nature of the personal data involved and the appropriateness of its retention period. The findings of the Commissioner are set out herein below.

Nature of the Incident

49. A data breach generally refers to a suspected or actual breach of the data security of the personal data held by a data user, resulting in the data affected by unauthorised or accidental access, processing, erasure, loss or use, thereby contravening the requirements of DPP4(1).

50. As evidenced by the information provided by Town Health in the Notification and Town Health's replies to various inquiries raised during the course of the investigation, the Commissioner came to the conclusion that the Incident was a data breach whereby the Medical Centre of Town Health accidentally disposed of a carton box containing personal data of 294 patients. The personal data included their names, telephone numbers,

Hong Kong Identity Card numbers, addresses, dates of birth, diagnosis records, medication records and laboratory results, etc.

Town Health Being the Data User in the Incident

51. The medical records in the Carton Box were collected by the Medical Centre, which is operated by Town Health. Town Health is therefore a data user as defined under section 2(1) of the Ordinance and is required to comply with the requirements of the Ordinance, including the six DPPs set out in Schedule 1 to the Ordinance.

Serious Deficiencies in Data Security

52. DPP4(1) stipulates that all practicable steps shall be taken by a data user to ensure that any personal data held by the data user is protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to –

(a) the kind of data and the harm that could result if any of those things should occur;
(b) the physical location where the data is stored;
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
(e) any measures taken for ensuring the secure transmission of the data.

53. Having considered the facts of the Incident and the evidence obtained during the course of the investigation, the Commissioner found that Town Health had serious deficiencies in terms of staff awareness, policy and staff training, which contributed to the accidental disposal of the Carton Box.

(1) *Lack of staff awareness of data protection*

54. The Commissioner considered that the two single events below served as the causes of the Incident: -

(i) HCA placed the Carton Box in the working area near a trash bin; and

(ii) The Cleaner treated the Carton Box as waste and disposed of it.

55. Human factors always play a significant role in data breaches. The Commissioner considered this Incident to be of no exception. In the Incident, both the HCA and the Cleaner apparently lacked the required awareness of data protection, and recklessly handled medical records of sensitive nature.

56. As a routine duty, the HCA handled a large amount of medical records in the Medical Centre. For the sake of work convenience, she paid less attention to the importance of personal data security in handling sensitive personal data. She had neither placed the Carton Box containing medical records of 294 patients properly (e.g. by keeping the Carton Box closed and putting it in a more discreet location, or even putting it into a locked cabinet) nor affixed any labels to the Carton Box to indicate the contents therein and their purposes when suspending the process of inspecting "Inactive Medical Records". Worse still, she placed the Carton Box near a trash bin that totally ignored the importance of the personal data placed therein. Such an act was also the consequential reason for the Incident. During the course of the investigation, Town Health admitted that the location (i.e. the area near the trash bin) was not an appropriate place to put the Carton Box at the material time. The above reflected the rash attitude of the HCA on data protection.

57. Furthermore, the Medical Centre had just completed renovation works the day before the Incident. It was expected that the HCA should have paid extra attention to the security of the Carton Box. Instead, the HCA apparently disregarded the risks and placed the Carton Box at will, to the extent that it misled the Cleaner to believe that the Carton Box was disposable.

58. Further, the Cleaner disposed of the Carton Box as waste simply because it was placed near a trash bin. According to the CCTV footage, the Carton Box was left open. The Cleaner should have checked with the relevant staff before disposal if he had noticed that the Carton Box contained documents.

(2) *Lack of effective policies and procedures*

59. All data users who collect and retain personal data should develop risk management policies, conduct due diligence and data privacy impact assessments to ensure that potential risks and situations that may lead to unauthorised or accidental loss or use of data should be identified, take reasonably practicable steps, and implement appropriate security policies and measures to reduce these risks.

60. Town Health is a sizable medical service provider, operating over 100 medical centres in the community, and regularly possesses and handles a large amount of sensitive medical data of patients. To fulfil the expectation of patients and stakeholders, Town Health should formulate comprehensive policies and procedures on the protection of medical records of patients. Nevertheless, during the course of the investigation, the Commissioner found that Town Health was well below par in this regard.

61. During the course of the investigation, although Town Health furnished the Commissioner with three sets of guidelines covering some requirements on the protection of medical records of patients, the contents of which were obviously not comprehensive and specific enough to prevent the Incident. The reasons are as follows: -

62. Town Health provided the guidelines for frontline staff on their handling of personal data of customers and the guidelines on handling, use and storage of medical records. The Commissioner noted that the two guidelines failed to set out specifically the security measures and work practices that should be adopted for the review of "Inactive Medical Records", but only included some generic requirements:

> A set of guidelines from Town Health to frontline staff on their handling of personal data of customers provided that: "*before leaving the workstation, you should ensure that any customer information has been properly stored (e.g. patients' data needs to be reversed or covered) in order to prevent the information from being accessed by third parties or outsiders easily*"[6].

63. The Commissioner considered the aforementioned guidelines were unclear and unspecific. For example, in the present case, was placing the Carton Box near the trash bin considered to be appropriate? During the course of the investigation, Town Health told the Commissioner that the HCA did not violate any guidelines in the Incident. Therefore, the Commissioner is convinced that no matter how well the aforementioned guidelines had been communicated to the frontline staff of the Medical Centre, it would not have prevented the occurrence of the Incident.

64. Meanwhile, the Commissioner considered that the "*Cleaning Guidelines*" were standard operating procedures of Town Health, but the content was

[6] Translation from the original Chinese text.

unclear. Even if the Cleaner had acted in accordance with the guidelines, this Incident might not necessarily have been prevented.

65. The Commissioner considered that the Incident might have been avoided if the "*Cleaning Guidelines*" had clearly listed out the types of items prohibited from disposal, and defined the criteria for the items to be considered disposable waste, such as the storage location or any identifiable label.

(3) *Lack of staff training*

66. During the course of the investigation, Town Health admitted that no training on personal data protection had been provided for its frontline staff.

67. The Commissioner considered that it is the duty of all data users to provide training for employees who are required to handle personal data as one of the measures in personal data protection. This is especially essential for Town Health as it has to handle sensitive medical data. Therefore, the Commissioner considered that the failure of Town Health to provide adequate training on the protection of personal data for the frontline staff was another critical factor contributing to the Incident.

Data Retention

68. Once personal data is collected, the data user will have to consider, *inter alia*, how long the personal data should be kept, as unnecessary and excessive period of retention of personal data would inevitably create or increase the risk of data breach.

69. According to the information provided by Town Health, the Carton Box was about to be transferred to the central warehouse of Town Health for

storage. The medical records contained therein belonged to 292 patients who had not visited the Medical Centre for more than seven years and two other patients who had their last visit in 2019.

70. Given that patients might seek medical treatment again or request for their medical records, the Commissioner considered it would generally be necessary for medical institutions to keep medical records for a longer period of time. Overall, the Commissioner considered that there was no information in this case suggesting that Town Health had kept the medical records concerned in the Incident for a prolonged period of time. Town Health **did not contravene** the requirements of DPP2(2) in Schedule 1 to the Ordinance as regards the retention of personal data.

Data Breach Notification

71. Whilst there is no statutory requirement under the Ordinance prescribing a data user to notify the Commissioner and the data subjects for data breach incidents, or the period within which such notifications are required to be made, the Commissioner noted that Town Health notified the Commissioner of the Incident on 2 June 2021 and took subsequent steps to inform the data subjects (i.e. the affected patients).

72. However, taking account of the sensitive nature of the personal data involved in the Incident (i.e. medical records), the Commissioner considered that Town Health should have lodged the Notification earlier. **The Commissioner regretted to note that Town Health only lodged the Notification nearly three months after the Incident.**

Conclusion – Contravention of DPP4(1)

73. The Commissioner considered that since medical records were sensitive personal data, Town Health, being a data user managing hundreds of medical centres and possessing a large number of medical records of

citizens, should devise comprehensive policies as to the collection, holding, processing and use of the medical records, conduct appropriate risk assessments, provide adequate training for its staff to instil data protection awareness, and take all practicable security measures in accordance with DPP4(1) to prevent any personal data held by it from unauthorised or accidental access, processing, erasure, loss or use.

74. The serious deficiencies in personal data protection of Town Health led to the otherwise avoidable disposal by accident of the Carton Box containing medical records of patients of the Medical Centre. During the time when the Carton Box was transported from the Medical Centre to the refuse collection point at about 200 metres away, the medical records in the Carton Box were constantly in a state where the documents therein could be inspected or taken at will. Anyone could have an opportunity to obtain the medical records.

75. Having considered all relevant evidence and circumstances associated with the Incident, the Commissioner considered that Town Health:

(1) Failed to examine and assess the risk of human negligence, thereby resulting in the failure to take appropriate measures to address the risk arising from the lack of awareness of employees on data protection;

(2) Failed to devise clear and adequate data security policies and guidelines to protect sensitive personal data; and

(3) Failed to provide adequate training for all relevant parties on the proper handling of personal data.

76. **In the present case, the Commissioner found that Town Health had serious deficiencies in ensuring the security of personal data. The Commissioner considered that Town Health had not taken all practicable steps to ensure that the medical records in question be**

protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP4(1) concerning the security of personal data.

V. Enforcement Action

77. Having found that Town Health contravened DPP 4(1) of Schedule 1 to the Ordinance, the Commissioner exercised her power pursuant to section 50(1) of the Ordinance to serve an Enforcement Notice on Town Health directing it to take the following steps to remedy the situation and prevent recurrence of the contravention:

(1) Conduct a comprehensive review and update on all its written policies, and standard operating procedures/guidelines in relation to data protection, so as to provide its medical centres with specific policies and operating procedures/guidelines;

(2) Devise effective measures to ensure staff compliance with the revised written policies, and standard operating procedures/guidelines on data protection;

(3) Devise effective measures to monitor the compliance of staff or any third party responsible for the cleaning services of its medical centres with the requirements of the "*Cleaning Guidelines*";

(4) Provide training for staff members on data protection, record the training processes properly, and evaluate the level of participation of staff and the effectiveness of the training; and

(5) Provide documentary proof to the Commissioner within two months from the date of the Enforcement Notice, showing the completion of items (1) – (4) above.

78. Under section 50A of the Ordinance, a data user who contravenes the requirements of an Enforcement Notice commits an offence and is liable, on first conviction, to a maximum fine at level five (i.e. HK$50,000) and imprisonment of up to two years.

VI. Recommendations

Medical records are sensitive personal data and should be treated seriously

79. Regardless whether personal data is lost by accident, leakage or improper disposal, the potential harm to individuals should not be underestimated, in particular when sensitive medical records are involved. Medical record is an important asset of the healthcare industry, as it contains sensitive health and medical information of an individual. It is therefore crucial for medical service providers to ensure that medical records should be properly managed and handled throughout their lifecycle. This is not only to comply with the provisions of the Ordinance, but also to shoulder moral responsibility for patients.

80. In the present case, the Incident appeared to be an isolated case in which a medical institution accidentally disposed of more than 200 medical records of its patients. That said, upon investigation the Commissioner revealed that Town Health had serious deficiencies in safeguarding the security of personal data. If Town Health treated the Incident as an isolated event and did not take any improvement measures pinpointing to the root causes of the Incident to strengthen its data protection, data breach incidents in a more serious nature could occur anytime at any of its medical centres. Fortunately, Town Health paid considerable attention to the Commissioner's investigation of the Incident, by dedicating itself to improving the policies and procedures on data protection to prevent recurrence of similar incidents. The Commissioner was also pleased to note that Town Health has appointed a data protection officer to oversee matters related to its personal data privacy.

81. **The Commissioner recommends that organisations should establish and maintain a proper system for the responsible use and retention of personal data. A Personal Data Privacy Management Programme**

could assist organisations to effectively manage the lifecycle of personal data from collection to erasure, handle data breach incidents promptly, and to ensure due compliance with the Ordinance. Meanwhile, organisations should appoint Data Protection Officer(s) to monitor compliance with the Ordinance and report any issues to the senior management.

82. In addition to establishing effective policies and practices on data protection, data users should take steps to constantly monitor whether the policies and practices are duly observed by their employees, and provide them with comprehensive training in order to minimise human error. **The Commissioner recommends that organisations should holistically enhance employees' awareness of personal data protection and cultivate a personal data protection culture across the board. Organisations should provide employees with comprehensive training to incorporate personal data protection into their daily duties, with a view to reducing human error caused by a lack of awareness.**

83. While data breaches in the online world are becoming pervasive in the era of digital age, data breaches cannot be overlooked in the "offline" world. Town Health and all data users processing personal data in physical form should not only learn a lesson from the Incident, but also nip similar incidents in the bud. **The Commissioner recommends that organisations should adopt the same level of security measures for the relevant systems in processing personal data, whether they are computerised or in physical form. While adopting reliable systems and security settings to protect systems from cyberattacks, organisations should also allocate resources to strengthen security measures in protecting physical data.**

While lodging data breach notification is not punitive, data users should not evade their responsibilities under the Ordinance

84. The Commissioner noted that many data users were overwhelmed by an incident of data breach. There is no statutory requirement under the Ordinance prescribing a data user to notify the Commissioner and the data subjects for data breach incidents, or the period within which such notifications are required to be made. In fact, when the PCPD receives data breach notifications, we will provide data users with appropriate advice to help them respond to data breach incidents promptly and take appropriate measures and actions in a timely manner, with a view to minimising the loss and damage done to organisations and data subjects. The PCPD will also provide advice to assist data users in improving their systems and policies for handling personal data to prevent the recurrence of similar incidents. On the contrary, delay in processing or notifying the Commissioner of a data breach may result in multiplied or irreversible damage to organisations and data subjects, including both emotional and actual financial harm. **The Commissioner recommends that when data users suspect or note the occurrence of a data breach incident, they should notify the PCPD as soon as possible. The PCPD will provide assistance and advice to help minimise the damage caused by the data breach incident and improve the personal data system.**

85. The PCPD has been working with the Government on concrete proposals in amending the Ordinance, including the setting up of a mandatory data breach notification mechanism. The PCPD will continue to carry out its duties in a proactive manner, with an aim to better protect the personal data privacy of members of the public.

— End —