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

Investigation Report:

Hospital Authority's Breach of Data Security in Connection with Disposal of Patient Records

Report Number: R13 - 6740

Date issued: 24 October 2013

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Investigation Report: Hospital Authority's breach of data security in connection with disposal of patient records

This report in respect of the investigation carried out by the Privacy Commissioner for Personal Data (the "**Commissioner**") pursuant to section 38(b) of the Personal Data (Privacy) Ordinance, Cap. 486 (the "**Ordinance**") against Hospital Authority ("**HA**") is published in the exercise of the power conferred on the Commissioner by Part VII of the Ordinance. Section 48(2) of the Ordinance provides that "*the Commissioner 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."

ALLAN CHIANG
Privacy Commissioner for Personal Data

Investigation Report: Hospital Authority's breach of data security in connection with disposal of patient records

The Privacy Commissioner has served an Enforcement Notice on the Hospital Authority as it has contravened Data Protection Principle 4 of the Ordinance for having failed to take all reasonably practicable steps to ensure that patient's personal data were protected against accidental access.

Background

2. On 29 June 2012, the media reported that a passer-by found a damaged roll of thermal ribbon containing patients' personal data of Pok Oi Hospital ("**POH**"), a hospital under HA's purview, lying abandoned on Kui Sik Street, Fanling, outside the shredding factory of Confidential Materials Destruction Service Limited ("**CMDS**"). CMDS was HA's waste disposal service provider. This Office initiated an enquiry against HA into the incident. Based on the photos taken by the media, HA conducted internal verification and informed this Office that the roll of thermal ribbon in question would have carried the image of 16 patients' personal data including their names, Hong Kong Identity Card numbers, dates of birth, gender, addresses and telephone numbers. HA notified the 16 patients by letters on 10 July 2012 of the incident.

3. On 3 September 2012, the media reported that the same passer-by found shredded strips of medical appointment slips from Our Lady of Maryknoll Hospital ("**OLMH**"), another hospital under HA's purview, lying abandoned in the same area outside CMDS' shredding factory. From the photos of the strips taken by the media, HA could not confirm the identity of patient(s) affected, but it estimated that the shredded pieces were approximately 16mm in width. A medical appointment slip typically contains a patient's name, gender, age and partial Hong Kong Identity Card number.

4. Consequently, the Privacy Commissioner decided to initiate an investigation into two data leakage incidents ("**Incidents**") against HA (the data user).

Relevant Provisions of the Ordinance

5. Of relevance to this investigation is Data Protection Principle 4 ("**DPP4**") in Schedule 1 to the Personal Data (Privacy) Ordinance (the "**Ordinance**")[1] and section 65 of the Ordinance. DPP4 provides that:-

"*All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other 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 are stored;
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are 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."

6. According to section 2 of the Ordinance, "practicable" means reasonably practicable.

7. Section 65(2) of the Ordinance stipulates that:-

"*Any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of this Ordinance as done or engaged in by that other person as well as by him.*"

[1] The Personal Data (Privacy) Ordinance was substantially amended on 1 October 2012. However, for the purposes of this investigation, the applicable law at the material time was the version of the Personal Data (Privacy) Ordinance prior to 1 October 2012, which is referred to as the "Ordinance" throughout this report.

Information collected during the Investigation

8. In the course of investigation, this Office made enquiries with HA (the date user) and CMDS (the contractor) and examined the documentary evidence provided by the two organisations. Below is the relevant information obtained by this Office.

Statutory Role of HA

9. As stipulated in section 4(c) of the Hospital Authority Ordinance, HA shall manage and develop the public hospitals system in ways which are conducive to achieving a number of objectives, such as to improve the efficiency of hospital services by developing appropriate management structures, systems and performance measures; and to ensure accountability *to the public for the management and control of the public hospitals system.*

Contract between HA and CMDS

10. CMDS provides waste collection and destruction services to 42 hospitals/institutions in Hong Kong, including POH and OLMH, under a contract between HA and CMDS effective from 1 November 2009 (the "**Contract**")[2].

Three categories of wastes

11. According to the Contract, wastes to be collected from hospitals and handled by CMDS are divided into three categories:-

[2] CMDS provided this Office with a copy of the Contract which covered a period of 24 months effective from 1 November 2009. The Contract has been repeatedly renewed since, for periods of either 4 or 6 months, on 1 November 2011, 1 March 2012, 1 June 2012 and 1 December 2012 respectively.

Category	*Materials containing personal data*	*Treatment*
A	**Waste paper classified as Confidential and Restricted (not to be disclosed to the public)**	For the collection of waste paper under Category A, CMDS would provide hospitals with serialised sealing safety devices / labels. Serial numbers provide a means for item verification between HA / hospitals and CMDS. During collection, collection bags are to be sealed securely in the company of hospitals' staff. Every serial number of the sealing device of the collection bag is recorded and signed for on a dispatch list by CMDS' collection staff. The dispatch list is subsequently checked and signed for by CMDS' shredding factory staff upon arrival of the waste bags. Waste paper should be shredded into strips not more than 4mm wide. After shredding, the waste paper would be transferred to CMDS' paper mills for recycling.
B	**Obsolete Forms/Booklets/Manuals**	Wastes should at least be cut into two halves. They would be transferred to CMDS' paper mills for recycling.
C	**Used Thermal Ribbons**	Used thermal ribbons should be shredded but the Contract does not detail the specification as to the width of the shredded strips. A senior officer of CMDS supplemented that the shredded ribbons would be disposed to landfills.

Relevant terms and conditions of the Contract

12. In relation to the two Incidents, the following terms and conditions of the Contract are relevant to an assessment on whether DPP4 has been complied with:

Quotation to invite supplier (part of the Contract)

1. Introduction

1.1 This quotation is issued to invite supplier for the provision of waste paper collection and destruction services to users from the hospitals … The list of hospitals under the Hospital Authority …
…

7. Submission of Monthly Report

The Contractor shall submit to all user hospitals a monthly report including the weight, categories, user departments …
…

Services requirement appended to quotation

…
4. The Contractor shall provide adequate clean nylon bags of different colours for various categories of Waste Paper (for example, green for Category A and blue for Category B) for easy identification and meet the demand of the users…
…

Waste Paper Handling Procedure

…
2. CMDS shall endeavor to collect all packed materials on the scheduled time and date. Should one collection run be inadequate, CMDS is to arrange for collection of remaining materials either on the same day or the following working day at the latest …

3. *We* [CMDS] *have a total number of 16 enclosed trucks to serve our clients. These trucks are equipped with Global Positioning System (GPS) to monitor daily operation routes.*

…

7. *Collected materials are transport*[ed] *to CMDS' owned Fanling workshop on the same day of collection…*

8. *Processing of collected materials shall be performed within 8 working hours after loading down at workshop… The shredding processes are monitored by CMDS personnel via 6 sets of CCTV; unauthorized entry to the workshop is prohibited.*

…

11. *All destroyed papers will be sent back to our own* [CMDS'] *China or Philippine Paper Mills for paper recycle only. The transportation process to China is handled by* [our] *own* [CMDS'] *ships & Trucks.*

…

Part III – Special Conditions of Contract

…

2. *Duties of the Contractor*

…

2.13 *The Authority may, upon request, inspect the shredding process at the Contractor's shredding factory and the Contractor shall provide the Authority* [HA] *(including its agents and representatives) all reasonable cooperation and assistance in relation to such inspection.*

…

2.15 *The Authority may conduct audits to review the Contractor's compliance with its obligations under this Contract including its obligations to protect the confidentiality of the Waste Paper and its compliance with applicable laws and regulations on data protection. The Contractor shall provide to the Authority* [HA] *(including its agents and representatives) all reasonable cooperation and assistance in relation to such audit.*

...

Interview with a senior officer of CMDS

13. A senior officer of CMDS gave evidence at an interview in February 2013 on CMDS' behalf. CMDS denied responsibility for the two Incidents. Regarding the Incident of POH's thermal ribbon, CMDS remarked that it had no record of ever having collected any Category C waste (used thermal ribbons) from POH since the commencement of the Contract in November 2009.

14. In respect of the Incident of OLMH's medical appointment slip strips, CMDS asserted that these could not have been processed by them since the strips, as shown in the photos taken by the media, were more than 4mm in width, which did not match the 4mm requirement laid down in the Contract.

15. CMDS had approached the media organisation in an attempt to retrieve the wastes in both incidents, but the media organisation had not responded.

16. Following the incidents, CMDS had installed a CCTV outside the factory in October 2012 to provide surveillance of the area where the roll of used thermal ribbon and strips of medical appointment slips were allegedly found. CMDS confirmed that no further abandonment of hospital wastes was reported after installation of the CCTV.

Submissions by HA

17. HA confirmed that POH's thermal ribbon as well as OLMH's medical appointment slips in question were amongst the items collected by CMDS under the Contract, and accepted that it was the data user responsible for the Incidents.

18. HA had not tried to approach the passer-by who found both items and the media which interviewed the passer-by and reported the incidents for return of the found items.

19. In an HA inspection of CMDS' shredding factory conducted on 5 October 2010, the HA team witnessed the shredding process of thermal ribbon. The HA team observed that the materials were too soft to be smoothly shredded by the machine, a thermal ribbon was found to be "incompletely shredded".

20. Following the 3 September 2012 media report of the second incident (i.e. OLMH's medical appointment slip strips), HA conducted another site visit to CMDS' shredding factory on 26 September 2012 and had the following key observations:

(i) HA witnessed a thermal ribbon falling out of a collection bag of paper wastes in the course of shredding. A CMDS worker immediately picked it up and separated it for non-paper shredding; and

(ii) HA witnessed paper wastes from a collection bag being fed into a shredding machine for shredding into 16mm wide strips instead of no more than 4mm wide as required under the Contract. HA was concerned whether this was the reason for the second Incident of leakage of the approximately 16mm wide shredded strips of OLMH's medical appointment slips. According to CMDS, the 4mm shredding machine was pending repair on the day of HA's visit. A newly recruited staff mistakenly fed the paper wastes into the 16mm-strip shredding machine adjacent to the 4mm-strip shredding machine. To avoid similar mistakes in future, CMDS has since clearly marked the area designated for processing wastes by 4mm shredding, placed a sign stating "Hospital Authority" on materials collected from HA and trained all their workers on the proper work procedure.

21. Having examined the monthly reports submitted by CMDS to POH from August 2011 to July 2012 and those submitted by CMDS to OLMH from November 2011 to October 2012, this Office found the reports show only the serial numbers of bags/boxes of wastes collected, but no information as to the categories of wastes collected as specified by the Contract. HA admitted that information on categorisation of wastes had been omitted from CMDS' monthly reports for all the hospitals.

22. After the Incidents, HA issued a written instruction on 29 November 2012 to all clusters which stated, among other things:

(i) HA and CMDS had held a meeting at which CMDS pointed out that HA's hospitals had "*sometimes*" placed all three categories of wastes together in the same collection bag; and

(ii) to facilitate shredding arrangements effectively (i.e. slower shredding speed for thermal ribbons for better shredding results) at the request of CMDS, HA instructed the hospitals to place Categories A and B wastes together in one bag and Category C wastes in a separate bag.

23. Under the Contract, both HA and its hospitals are entitled to inspect the shredding process at the CMDS shredding factory. HA Head Office itself did not conduct such inspection on a regular basis. Indeed, only one inspection was conducted on 5 October 2010 in the two years and seven months since the Contract took effect and before the first Incident. During the same period, only seven of the 42 hospitals had conducted inspections. HA Head Office had initially denied that they were responsible for centrally monitoring inspections conducted by the hospitals of CMDS' shredding factory. HA Head Office had not issued any policy or guideline to the hospitals on conducting inspection. They had not reviewed any record of inspections conducted by the hospitals.

24. Later, on 24 May 2013 HA supplemented that commencing May 2013 their internal working group on municipal waste management would conduct annual site inspections. Inspection team members would comprise representatives from all clusters and HA Head Office. Also, each cluster is required to conduct annual site inspection focusing on the physical security controls of the collection, delivery and the shredding processes. The working group would examine all the inspection findings to assess CMDS' compliance with the Contract.

25. Under the Contract, HA may conduct audits to review CMDS' compliance with its obligations under the Contract including its obligations "to protect the confidentiality" of the paper wastes and its compliance with applicable laws and regulations on data protection. However, HA admitted that they had never carried out such audit.

The Commissioner's Findings

HA's responsibility for the two Incidents under DPP4

26. CMDS denied responsibility for the two Incidents, for explanations given at paragraphs 13 and 14 above. The Commissioner held that its explanations hardly stand up to scrutiny.

27. As regards the first Incident, CMDS pointed out that it had no record of having received Category C wastes (see paragraph 13). Admittedly, although categorisation of wastes is specified under the Contract, CMDS' monthly reports to HA's hospitals do not in fact provide information by category on the wastes processed for that hospital. However, no entry of Category C waste did not necessarily mean there was no collection of Category C wastes. First, on both rare inspections conducted by HA at CMDS' shredding factory, thermal ribbons were found (see paragraphs 19 and 20(i)). Further, CMDS' own feedback to HA (which led to HA's instruction on 29 November 2012 to all clusters) acknowledges that sometimes all three categories of wastes were placed in the same collection bag (see paragraph 22(i)) for CMDS' processing.

28. As regards the second Incident, CMDS' explanation was that it could not be responsible because OLMH's medical appointment slip strips in question were 16mm in width which far exceeded the output width of 4mm for paper waste after due shredding. This assertion is refuted by HA's evidence of having witnessed at the inspection on 26 September 2012, hospital paper wastes being incorrectly fed by CMDS staff into a shredding machine for shredding into 16mm instead of 4mm wide strips (see paragraph 20(ii)). Apart from indicating that CMDS had plainly failed to process Category A wastes in conformity to the required standard, CMDS' explanation also reflected that their staff were insufficiently trained and that the physical setting of the shredding area was not conducive to staff choosing the correct type of shredding machine for handling hospitals' paper waste.

29. On the basis of the above, the Commissioner is of the view that the abandoned waste items in the Incidents, namely, POH's thermal ribbon and OLMH's medical appointment slip strips, were in all likelihood items that had been processed by CMDS at its Fanling factory. How these shredded wastes were abandoned on the street is yet unknown. They could have been taken

away from the workshop in an unauthorised manner or accidentally lost during transit to the landfills or CMDS' paper mills.

30. By virtue of section 65(2) of the Ordinance, any act done or practice engaged in by an agent for another person with the latter's authority, shall be treated as done or engaged in by both the agent and that other person. For this reason, even though HA had entrusted CMDS with the task of hospital waste collection, destruction and disposal, as data user HA remains accountable for any unauthorised or accidental access of personal data contained in the abandoned waste in these Incidents. In any event, HA admitted liability for the Incidents (see paragraph 17 above).

Whether all practicable steps taken to ensure protection of personal data

(i) ***Contractual omission in treatment of thermal ribbon***

31. Security measures are found in the Contract in relation to the processing of paper wastes containing patients' personal data which are classified as Category A wastes. Such wastes are to be placed in serialised sealing safety devices for collection, and then shredded into strips no wider than 4mm.

32. The Incident involving POH's thermal ribbon shows that Category C wastes similarly contain sensitive personal data of patients such as their Hong Kong Identity Card numbers, dates of birth and contact details. However, the Contract is completely silent on the appropriate measure to safeguard the personal data contained in such non-paper wastes such as the use of serialised sealing safety device or specifying the maximum width of shredding.

33. In this connection, the Commissioner pointed out that HA had at an inspection conducted on 5 October 2010 of CMDS' factory, observed that a thermal ribbon was "incompletely shredded". It is unclear what HA meant by "incompletely shredded" but conceivably, the personal data of a completely shredded ribbon should not be readily recognised or recovered. A proper specification in the Contract would at least provide a contractual guarantee that no issue of personal data security will arise even if a properly shredded ribbon was taken away from the factory without authority or accidentally lost in transit, as it might have happened in the Incident. Regrettably, this is omitted in the Contract.

(ii) Contract Management

Inadequate supervision of contractor

34. Except for this major omission, the Contract could be an effective means for HA to discharge its obligations as a data user under DPP4, if it had managed the Contract competently.

35. As noted in paragraph 9 above, one of the statutory roles of HA is to ensure accountability to the public for the management and control of the public hospitals system.

36. As noted in paragraph 23, under the Contract, HA and its hospitals are entitled to inspect the shredding process at CMDS' factory.

37. If coordinated well and conducted as well as followed up properly, inspection is an effective tool to check the performance of the data processor and identify irregular practice for prompt rectification.

38. However, HA Head Office denied responsibility for centrally monitoring the inspections carried out by hospitals. In our investigation it was found that no guideline or coordination existed between HA and hospitals as to any defined frequency, scope or reporting requirement for such inspections. Instead, hospitals decided on their own whether and how to conduct the inspection, and HA neither received nor asked to review the hospitals' inspection reports.

39. HA Head Office itself had conducted infrequent inspections of CMDS' factory - twice so far - but even these two rare inspections have identified key problems, namely, "incomplete shredding" of both the thermal ribbon and the confidential paper waste (see paragraphs 19 and 20 above). But for such incomplete shredding of confidential paper and ribbon wastes, the abandoned hospital wastes of the Incidents would be plain and meaningless wastes, without any associated risk of personal data security.

No audit

40. It is also noted that HA had not carried out any audit to review or verify if CMDS had in fact complied with its obligations under the Contract and requirements under the Ordinance. While an inspection would only identify irregularities in the CMDS shredding factory, an audit could include more comprehensive and in-depth examination of the whole handling process of HA hospital wastes that comprises waste segregation at the hospitals, collection by CMDS, transportation from hospitals to CMDS' shredding factory, the shredding process, and transportation of the shredded wastes from the factory to the landfills or paper mills.

41. HA had not made use of this contractual tool at all to assess comprehensively CMDS' performance of its contractual obligations in the handling of hospital wastes. Consequently, the Commissioner has managed to gather very little information from HA as to how CMDS has operated in practice. Against this background, it is no coincidence that the Commissioner has not been able to identify any clue to how the hospital wastes in the Incidents ended up abandoned on the street.

Conclusion

42. The precise cause leading to the abandonment of the hospital wastes on Kui Sik Street is still unknown. The leakage of the personal data in question was clearly an outcome of incomplete or improper shredding of the wastes. The mistake is attributable to CMDS but HA is ultimately accountable. The findings set out above indicate that the Contract between HA and CMDS is inadequate to ensure proper and complete shredding of thermal ribbons, and HA has not competently managed the Contract. On this basis, I conclude that HA had contravened DPP4 of the Ordinance for having failed to take all reasonably practicable steps to ensure patients' personal data were protected against unauthorised or accidental access.

Enforcement Notice

43. In view of the finding of contravention on the part of HA and that the underlying problems still persist, the Commissioner has decided to serve an Enforcement Notice on HA pursuant to section 50 of the Ordinance. The Enforcement Notice directs HA to :

Within 3 months after the date of service of the Enforcement Notice

(1) make reasonable endeavor to retrieve and destroy the abandoned hospital wastes identified in the two Incidents;

Within 4 months after the date of service of the Enforcement Notice

(2) review and revise the hospital wastes disposal process and implement at the minimum the following improvement measures : -

- separate hospital wastes containing personal data into paper wastes and non-paper wastes;
- specify by contractual or other means how to safeguard used thermal ribbons and to ensure they are shredded in a manner which prevent the personal data contained therein from being readily recognised or recovered;
- ensure all paper wastes with personal data are treated at Category A security level;
- review and revise CMDS' monthly report format to enable meaningful and effective monitoring;
- conduct comprehensive audit to cover the whole waste disposal process;
- conduct inspections of hospitals and CMDS' shredding factory at least once annually; and
- assume a central monitoring role in the hospitals' inspection of CMDS' shredding factory and promulgate to hospitals policies and guidelines in this regard.

Other Comments

44. Data users are obliged to protect personal data by reasonable security safeguards against such risks as loss, unauthorised access, destruction, use, modification or disclosure of data. This responsibility covers the complete data life cycle from data creation to final disposal.

45. The potential harm to individuals from the misuse of their personal data, whether accidentally lost, leaked or purposely stolen, could be significant, particularly in the case of patients when sensitive medical records are involved.

46. The unsatisfactory performance of CMDS as HA's contractor in the treatment of hospital wastes containing patients' personal data is unacceptable. Under the Ordinance, the Commissioner has no authority to regulate directly the work of CMDS as a data processor. The onus is on HA to use contractual or other means to secure CMDS' compliance with the relevant Ordinance obligations. Regrettably, HA's oversight of CMDS' performance, in terms of contractual and procedural rigour as well as physical supervision, is far from satisfactory. At this critical time when the Government is about to introduce the e-Health Record Sharing System which has serious privacy implications, the Commissioner sees that it is imperative for HA to measure up and demonstrate to the public its commitment to ensuring privacy and data protection.