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

Report Number: R08-1935

Date issued: 24 December 2008

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

Loss of Patient's Personal Data by United Christian Hospital

Case number: 200801935

This report in respect of an investigation carried out by me pursuant to section 38(a) of the Personal Data (Privacy) Ordinance, Cap 486 ("the Ordinance") against United Christian Hospital ("UCH") of the Hospital Authority ("HA") is published in the exercise of the power conferred on me 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."

Roderick B. WOO
Privacy Commissioner for Personal Data

(Note: This is an English translation of the Report compiled in Chinese.)

The Case

The Complainant said that she had received psychiatric treatment at Ngau Tau Kok Maternal and Child Health Centre on 24 August 2007 and given her personal data to a psychiatric nurse, Nurse X. On 25 January 2008, the Complainant received a call from Nurse Z of UCH, informing her that UCH found on 17 January 2008 that a USB flash drive ("USB") containing her personal data (including name, Hong Kong Identity ("ID") card number, residential address and contact telephone number) was lost. Nurse Z also told the Complainant that personal data of a total of 23 ladies were lost and UCH had reported the case to the police on 18 January 2008.

2. In this connection, the Complainant complained that UCH had lost her personal data.

Relevant Provisions of the Ordinance

3. Data Protection Principle ("DPP") 4 in Schedule 1 to the Ordinance is relevant to this case:

> *"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."*

4. According to section 2(1) of the Ordinance, "*practicable*" means

"reasonably practicable".

Information Collected during the Investigation

5. In the course of the investigation, we had interviews with Nurse X and Dr. Y, Hospital Chief Executive of UCH, and took statements from them. Moreover, we received written replies and relevant documents from UCH in respect of the case. We have collected the following information which were relevant to the case.

Background

6. HA, in collaboration with the Department of Health, has provided the public with the Comprehensive Child Development Service ("CCDS") since February 2006. As psycho-social health service is also provided to postnatal mothers under CCDS, psychiatric nurses of UCH will be assigned to three Maternal and Child Health Centres in Kowloon East (i.e. Ngau Tau Kok, Lam Tin and Tseung Kwan O), the Obstetrics and Gynaecology Specialist Out-patient Clinic of UCH or the CCDS Office of the Yung Fung Shee Psychiatric Centre ("Yung Fung Shee") to provide the service.

7. Nurse X was assigned to work in the CCDS of UCH on 24 July 2007. Her main office was at Yung Fung Shee, but she would also be assigned to Ngau Tau Kok Maternal and Child Health Centre and other places to provide psycho-social health service to pregnant women and postnatal mothers.

8. Nurse X's daily routine included meeting patients, during which Nurse X needed to collect patients' registration data (including name, date of birth, ID card number, address and contact telephone number) and clinical consultation notes. Patients handled by Nurse X could be divided into two categories: patients who had registered at Yung Fung Shee or UCH belonged to the first category ("Category 1 patients"), while patients who had never registered at Yung Fung Shee or UCH belonged to the second category ("Category 2 patients"). As Category 1 patients had received service at Yung Fung Shee or UCH, Nurse X needed to input the clinical consultation notes of Category 1 patients into HA's Clinical Management System ("CMS") for medical purposes. Regarding Category 2 patients, as they had not been provided with HA's medical service and they were only patients under the CCDS, it was not necessary to input any of their data into HA's CMS.

However, as patients of both categories were patients under the CCDS, their registration data had to be stored in the master computer file of the CCDS at Yung Fung Shee, and hard copies of their clinical consultation notes had to be kept in patient files.

9. Therefore, in her daily routine, Nurse X had to bring the registration data collected at Ngau Tau Kok Maternal and Child Health Centre, one of her working places, back to Yung Fung Shee and store the data in the master computer file of the CCDS, and bring the clinical consultation notes back to Yung Fung Shee for printing and filing for case discussion during meeting. Prior to 10 October 2007, Ngau Tau Kok Maternal and Child Health Centre still had no computer system linking up with HA or Yung Fung Shee. After 10 October 2007, though CMS had been installed in Ngau Tau Kok Maternal and Child Health Centre, the system was only used for handling patients' data of HA and for other related purposes, not for storage of patients' data under the CCDS. Hence, on the first day when Nurse X reported duty at the CCDS (i.e. 24 July 2007), UCH gave her a USB ("the USB") for storage of clinical consultation notes, and transmission of registration data to Yung Fung Shee for inputting the data into the master computer file of the CCDS. According to Nurse X, when she was given the USB, UCH informed her verbally of the procedures and requirements for collection, storage and erasure of patients' personal data by USB (please see below for details).

10. Prior to 10 October 2007, when Nurse X finished meeting her patients at Ngau Tau Kok Maternal and Child Health Centre, she would store the registration data of patients of both categories and the clinical consultation notes of Category 2 patients in the password protected zone of the USB, while recording the clinical consultation notes of Category 1 patients on papers. When she went back to Yung Fung Shee, she would then input the registration data of patients of both categories into the master computer file of the CCDS, and the clinical consultation notes of Category 1 patients into HA's CMS. Before attending the weekly clinical meetings to discuss medical cases, Nurse X had to print the clinical consultation notes of patients of both categories from CMS and the USB for meeting and filing.

11. Regarding deletion of data, Nurse X was informed that she had to discuss medical cases in weekly clinical meetings and upon formal termination of service to a patient, the clinical consultation notes of the patient had to be immediately deleted from the USB. However, the registration data would still

be kept in the password protected zone of the USB. In case Nurse X was consulted about the condition of a patient by HA or other medical officers of the CCDS, she could give a reply according to the registration data stored in the USB.

12. Since 10 October 2007, Ngau Tau Kok Maternal and Child Health Centre had been installed with CMS linking with HA. Therefore, Nurse X could directly input the clinical consultation notes of Category 1 patients into the CMS at Ngau Tau Kok Maternal and Child Health Centre. However, she still needed to store the registration data of patients of both categories and the clinical consultation notes of Category 2 patients in the password protected zone of the USB, and bring them back to Yung Fung Shee, where she would input the registration data into the master computer file of the CCDS. The data would also be used for answering enquiries of other medical officers.

13. As Nurse X had to work at different places, she would bring the USB along and take it home after work. Only when Nurse X went to work at Yung Fung Shee, she would input the registration data into the master computer file. The clinical consultation notes of Category 2 patients whose service was not terminated were kept in the USB.

Loss of the Complainant's Personal Data

14. On 24 August 2007, Nurse X met the Complainant, who was referred by Ngau Tau Kok Maternal and Child Health Centre for psycho-social health service. The Complainant belonged to Category 1 patient so Nurse X simply stored the registration data of the Complainant in the password protected zone of the USB. Some time later on the same day, Nurse X terminated the service to the Complainant. As mentioned in paragraph 11 above, the registration data of the Complainant was still kept in the password protected zone of the USB.

15. In mid October 2007, Nurse X found that the password protected zone of the USB was defective and she could not access the data in that zone, but she had not reported the case to her supervisor immediately. In order to continue her duty, Nurse X copied the registration data of all the 26 patients (including the Complainant) handled by her since 27 July 2007 from the master computer file at Yung Fung Shee to the non password protected zone of the USB. During the period from the discovery of the defect of the password

protected zone of the USB to the loss of the USB, no data of any new patient was added to the USB. In other words, the personal data lost in the case included the registration data of those 26 patients (including the Complainant) and the clinical consultation notes of some patients stored in the password protected zone of the USB.

16. On 20 October 2007, when Nurse X went back to Yung Fung Shee, she found that the USB had been lost, but she was not sure when, under what circumstances and how this had happened. In response to our enquiry, Nurse X said that the last date she had used the USB was 17 October 2007. She remembered that she had worked at Yung Fung Shee, the Obstetrics and Gynaecology Specialist Out-patient Clinic of UCH and Ngau Tau Kok Maternal and Child Health Centre on 18 October 2007, but she forgot her work location on 19 October 2007 (public holiday). After Nurse X had found that the USB was lost, she tried in vain to search for it. Therefore, on 17 January 2008, she reported the loss to her supervisor. UCH then reported the case to the police the next day. Since noticing the loss of the USB, Nurse X had stopped using USB to handle or store patients' personal data. Instead, she brought or faxed the papers containing the registration data to Yung Fung Shee, and stored the clinical consultation notes in the intranet email account provided by HA.

UCH's Internal Guidelines or Procedures on the Use of USB

17. UCH provided us with copies of the following documents to show that it had in place the internal guidelines on the use of USB:

(a) "Clinical Data Policy Manual – Section 3.5"
(b) "Information Security Policy and Procedure – Section 6.6.1 – 6.6.2"
(c) "A Practical Guide to IT Security for Everyone Working in HA – P.9"
(d) Booklet on "Protect Patient Confidentiality"

18. Moreover, according to Dr. Y, UCH will provide training and seminars from time to time to familiarize its staff with the policies and guidelines of the hospital. Whenever UCH issues new or revised policies, internal guidelines and/or circulars, staff will be informed via the following four channels:

(1) Email

Before this incident, the management staff, doctors, nurses (including Nurse X), allied health staff and some other staff have been assigned an email account to receive the hospital's policies, internal guidelines and circulars.

(2) Document Copies

Copies of the newly issued or revised policies, internal guidelines and/or circulars will be circulated in different departments. It is the discretion of the departments to decide whether their staff need to acknowledge reading.

(3) Intranet

The newly issued or revised policies, internal guidelines and/or circulars will also be posted in the intranet. Staff can log on at any time without using a password to read or download the policies, internal guidelines and/or circulars.

(4) Screensaver function

UCH will remind its staff of the newly issued or revised policies, internal guidelines and/or circulars via the screensaver function of the hospital's computers.

19. However, Nurse X said that apart from informing her verbally of the procedures and requirements for collection, storage and erasure of patients' personal data by USB, UCH had not provided her with any training, circular or guideline on the handling of patients' personal data by USB or other portable electronic storage devices. UCH provided her with relevant training, seminars and internal circulars only until May 2008.

20. Moreover, Dr. Y expressed that UCH had not rigidly set the time for reporting to the hospital when a staff member lost patients' personal data, but staff could report different kinds of incidents at any time via the "Advanced Incident Reporting System". Nurse X also reported the loss of the USB via this system on 18 January 2008.

21. Dr. Y confirmed that UCH had not regularly checked the use of USB by its staff in handling patients' personal data. But after this incident, all staff

were forbidden from using USB to handle patients' personal data, unless application had been made to him and approval was granted. However, he received no application for the use of USB from staff.

Remedial Actions taken by UCH

22. In respect of this incident, UCH has taken a series of remedial actions, which include:

(1) Since 19 January 2008, UCH had recalled all the USB given to the nurses of the CCDS and deleted all the patients' data inside.

(2) From 23 to 28 January 2008, the nurse-in-charge of the CCDS office called the patients involved to explain the incident and make apologies, and met with the Complainant on 30 January 2008.

(3) The officer-in-charge of the psychiatric unit of UCH and the nurses of the CCDS held a meeting on 22 January 2008 to discuss the improvement measures. The meeting passed a motion that intranet email account and facsimile would be used to store and transmit the personal data of patients of the Maternal and Child Health Centre, instead of using USB to store and transmit patients' data.

(4) An investigation panel was set up on 25 April 2008 by UCH to identify the cause of the incident and the room for improvement. To ensure impartiality and transparency of the investigation, UCH invited a member of its Hospital Governing Committee and a member from the Health Informatics section of HA Head Office to take part in the investigation.

(5) On 7 May 2008, HA's Chief Executive issued an email to all staff of HA, requesting them to safeguard all the devices containing patients' personal data, encrypt and password protect all the files containing patients' personal data, and ordering that without written approval of the Hospital Chief

Executive, staff were not allowed to bring USB containing patients' personal data away the precincts of HA.

(6) On 14 May 2008, HA also issued an internal circular, "Hospital Authority Head Office Information Technology Circular No. 1/2008 – Enhanced Measures on Enforcing Personal Data Security", to enhance the security measures on the protection of patients' personal data.

(7) On 15 May 2008, HA issued another internal circular, "Hospital Authority Head Office Operation Circular No. 9/2008 – Policy on the Management of Loss of Electronic Devices Concerning Patient Identifiable Personal Data", directing staff that once electronic storage devices containing patients' personal data were found lost, they had to report the loss immediately, and listing out the reporting procedure.

Result of the Investigation

23. This case involved the procedures for handling patients' personal data. As a public medical service provider, UCH handles huge amount of patients' personal data which are of sensitive nature. Therefore, it should take more stringent measures to safeguard patients' personal data.

24. In the circumstances of the case, UCH needs to comply with DPP4 to take all practicable steps to ensure that personal data of the patients (including the Complainant) held by it are protected against unauthorized or accidental access, processing, erasure or other use. This investigation was focused on whether sufficient safeguards had been taken when UCH provided its staff with USB for handling and storage of patients' personal data. The relevant issues derived from the complaint were whether UCH had appropriate policies and guidelines in place to inform its staff to protect patients' personal data when its staff were allowed to use USB for handling and storage of such data, and whether UCH had related measures to ensure compliance with the policies and guidelines by its staff.

25. According to UCH and Dr. Y, UCH did provide training and seminars to familiarize all staff with its policies and internal guidelines. UCH will use different ways to inform its staff of the newly issued or revised policies,

internal guidelines and/or circulars. Therefore, copies of the documents mentioned in paragraph 17 above should have been provided to its staff (including Nurse X) for information. However, according to Nurse X, UCH had only informed her verbally of the procedures and requirements for collection, storage and erasure of patients' personal data by USB. Prior to the incident, she had never seen any guidelines on the protection of patients' personal data privacy nor received any training on the use of USB or other portable electronic devices from UCH. If UCH did provide Nurse X with the relevant policies, guidelines and/or circular via the above mechanism, Nurse X's statement revealed that there were problems in the dissemination of information via the mechanism.

26. Furthermore, even if, as UCH and Dr. Y said, the hospital had put in place the policies or internal guidelines on the use of USB or other portable electronic devices, and provided its staff (including Nurse X) with the relevant policies or internal guidelines, but upon scrutinizing the related documents, I found that the relevant policies or internal guidelines only reminded staff in a general way that they should be careful when handling patients' personal data with electronic devices. For example:

> "Clinical Data Policy Manual – Section 3.5"
>
> "*Guidelines*
>
> *Since exporting patient data may increase the possibility of breach of confidentiality, intentionally or inadvertently, data exports should be avoided as far as possible"*
>
> "Information Security Policy and Procedure — Section 6.6.1"
>
> "***Removable computer media should be controlled.***
> …
> *4. Store all media in a safe, secure environment, in accordance with manufacturers' specifications."*
>
> Booklet on "Protect Patient Confidentiality" - Section IV
>
> "*General Principle*

All stored personal information, whether in hard copy, any types of computers, laptop, home-based PC or any other medium, should be protected from unauthorized or accidental access, processing, erasure or other use through the use of appropriate security devices and functions.

…

What you shouldn't do:

…

✗ *leave floppy discs, tapes, CD Roms and other types of media lying around unattended in a non-secure place"*

However, I did not find that before 14 May 2008, UCH had any detailed instructions and application procedures on the use of electronic devices such as USB (including response measures for the loss of such devices) in place for compliance by its staff.

27. Moreover, as CMS and the CCDS had kept the registration data and clinical consultation notes of patients, in case Nurse X was enquired about the medical history of a patient, she could make direct reference to the files in CMS or the CCDS before giving a reply. Furthermore, the reply will be more accurate when it is made after a direct access to the files in CMS or the CCDS than relying on the registration data to recall the patient's condition. In this premise, I am of the view that Nurse X had no need to keep the registration data which had been transmitted to the computer file of the CCDS in the USB. If Nurse X kept those registration data in the USB for her convenience at work, such act would not be proportional to the protection of patients' personal data privacy.

28. As UCH had not properly put in place any policy or internal guideline on the use of USB, Nurse X, without any actual needs, still kept the registration data in the USB. When she found that the password protected zone of the USB was defective, not only did she not report the case to her supervisor immediately, but she continued to use the USB by storing patients' personal data in the non password protected zone. Similarly, when Nurse X found on 20 October 2007 that the USB had been lost, she did not report the case to the hospital immediately.

Conclusion

29. In view of the above, I found that UCH had not taken all practicable steps to safeguard the personal data, causing the loss of the personal data of the 26 patients (including the Complainant), contrary to DPP 4.

Enforcement Notice

30. Pursuant to section 50 of the Ordinance, I may serve an enforcement notice on HA if I am of the opinion that HA contravened DPP4 of the Ordinance in circumstances that make it likely that the contravention will continue or be repeated. In view of the fact that the staff of UCH had stopped using USB to store and transmit patients' data, there was no evidence before me that the contravention of UCH will likely to continue or be repeated. Hence, I have not served on HA an enforcement notice in consequence of the investigation.

Recommendations and Other Comments

31. I learnt that after the incident, UCH had forbidden its staff from using USB to handle and store patients' personal data (unless prior approval from the Hospital Chief Executive was obtained). Even if staff can continue to use USB to handle and store patients' personal data, HA has issued relevant internal guidelines and application procedures to staff of UCH.

32. Moreover, in the inspection report published by this Office on 22 July 2008 after the inspection of hospitals under HA, recommendations on the protection of patients' personal data have been made to help hospitals improve the handling of patients' personal data.

33. In the wake of the development of technology, the size of electronic storage devices is getting smaller while the capacity is increasing. As a result, the risk of losing such devices and the number of individuals affected by the losses are increasing. It is no doubt that technology advancement will bring convenience at work. However, when using technology to enhance work efficiency, data users should also raise the awareness and requirements of their staff in the protection of personal data, and revise the established policies and internal guidelines to keep pace with technological advance.

34. USB offers a wide range of uses and is portable. I believe that a lot of medical staff will use USB to store patients' personal data. But before using USB, medical staff should first consider if there is any actual need to use USB or there is any other substitute, and ponder the potential risk of using USB. In this case, the medical staff could in fact substitute intranet for USB, which could also minimize the risk and impact of losing patients' personal data. Of course, when transmitting data by electronic means of communication, the issue of security should also be taken into consideration. If after careful consideration, medical staff still find it necessary to use USB to store patients' personal data, they shall adopt effective measures to protect the personal data against unauthorized or accidental access, processing, erasure or other use. For example, patients' personal data stored in USB should be encrypted; once the encryption function of a USB is found defective, the use of the USB should be stopped without delay; patients' personal data should be deleted from USB immediately after use; and whenever a USB containing patients' personal data was found missing, medical staff should promptly report the case to the relevant parties.