Report Published under Section 48(1) of the Personal Data (Privacy) Ordinance (Cap. 486)

根據《個人資料（私隱）條例》（第 486 章）第 48（1）條發表的報告

Report Number: R08-4232

報告編號：R08-4232

Date issued: 22 July 2008

發表日期：2008 年 7 月 22 日

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

Report on the Inspection of the Hospital Authority's Patients' Data System

This report of an Inspection carried out by me pursuant to section 36 of the Personal Data (Privacy) Ordinance, Cap. 486 (hereinafter referred to as "the Ordinance") in relation to the Hospital Authority is published in the exercise of the power conferred on me by Part VII of the Ordinance.

Section 36 of the Ordinance provides that :

> *"Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of –*
>
> *(a) any personal data system used by a data user; or*
>
> *(b) any personal data system used by a data user belonging to a class of data users,*
>
> *for the purposes of ascertaining information to assist the Commissioner in making recommendations –*
>
> *(i) to-*
>
> *(A)…*
>
> *(B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and*
>
> *(ii) relating to the promotion of compliance with the provisions of the Ordinance, in particular, the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be."*

The term, **"personal data system"** is defined in section 2(1) of the Ordinance to mean *"any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system".*

The Hospital Authority belongs to the class of data users who provide health-care services.

Section 48(1) of the Ordinance provides that: "*Subject to subsection (3), the Commissioner may, after completing an inspection where section 36 (b) is applicable, publish a report:*

(a) setting out any recommendations arising from the inspection 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

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

Subsection (3) states that: *"Subject to subsection (4), a report published under subsection (1) or (2) shall be so framed as to prevent the identity of any individual being ascertained from it".*

Subsection (4) provides that: *"Subsection (3) shall not apply to any individual who is*:

(a) the Commissioner or a prescribed officer;

(b) the relevant data user."

Roderick B. Woo

Privacy Commissioner for Personal Data
Hong Kong SAR

Table of Contents

CHAPTER ONE

Introduction

1.1 This report relates to the Inspection carried out by the Privacy Commissioner for Personal Data ("the Commissioner") pursuant to section 36 of the Personal Data (Privacy) Ordinance, Chapter 486 ("the Ordinance") in response to the recent numerous reported cases of loss of patients' personal data by various hospitals under the management of the Hospital Authority (hereinafter referred to as "HA"). The Commissioner was gravely concerned about whether the personal data system of the HA is adequate in ensuring the safety of patients' data and in compliance with the requirements of the Ordinance.

1.2 Relevant to the Inspection is the requirement prescribed by **Data Protection Principle 4** ("**DPP 4**") in Schedule 1 to the Ordinance which provides that:

> *"**PRINCIPLE 4 – SECURITY OF PERSONAL DATA***
>
> *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 the 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 that data."*

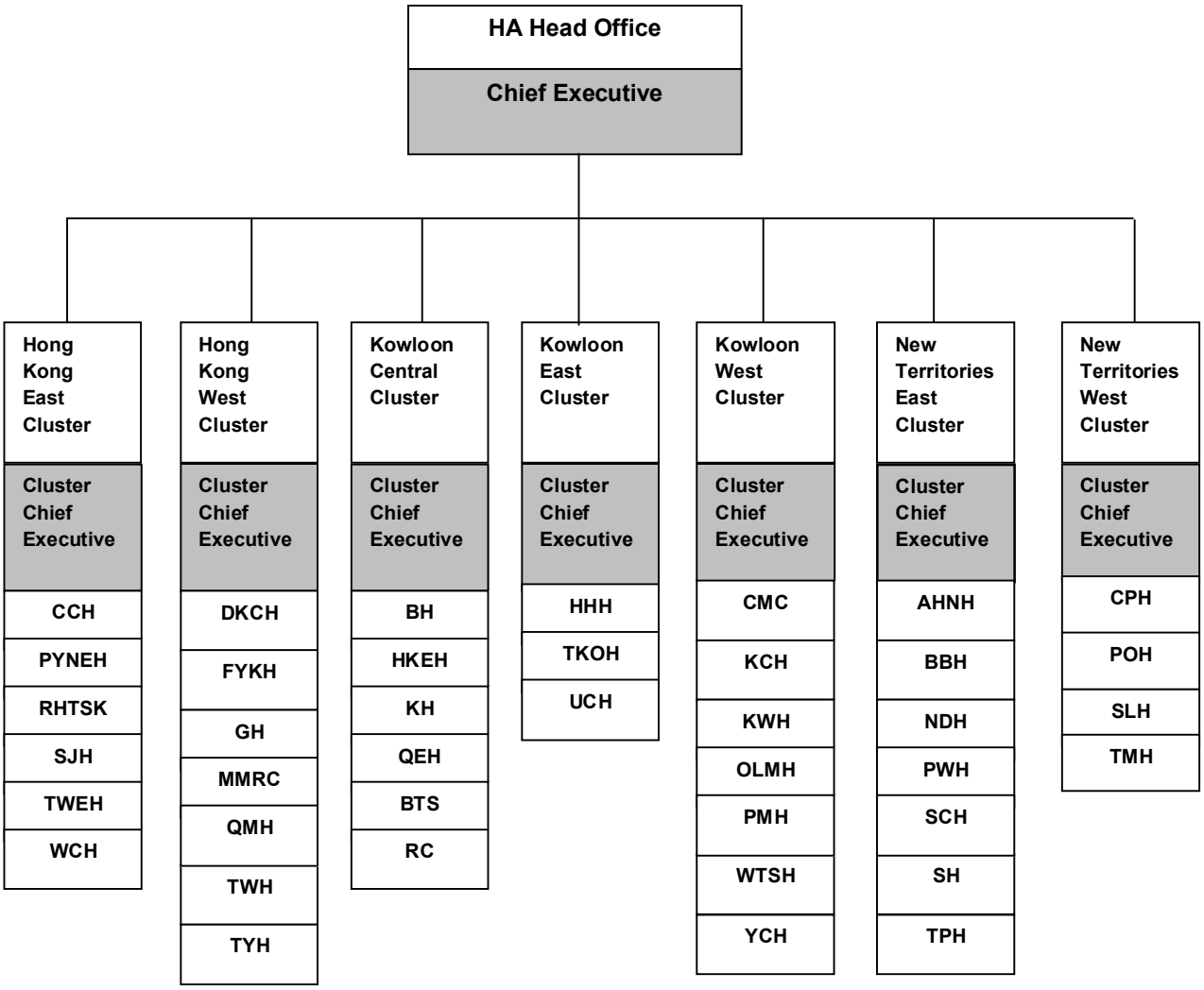
The term *"practicable"* is defined under section 2 (1) of the Ordinance to mean *"reasonably practicable."*

1.3 The medical data of a patient is generally regarded as being of particular sensitivity and accordingly, a user of such data has special responsibilities to safeguard their security. This is particularly so when the data user belongs to the class of health-care service providers whose everyday functions and duties involve the handling of substantial amount of patients' data. The loss or damage that may be caused to the data subjects (patients) as a result of any improper handling of their medical data can be serious and far-reaching. Hence, the HA should be mindful of the sensitivity of the data it holds and the risks of unauthorised access to ensure that the security precautions taken by it are reasonable, appropriate and effective in protecting them in compliance with DPP 4.

1.4 The HA is a statutory body which was established on 1 December 1990 under the Hospital Authority Ordinance, Cap.113, to manage the provision of hospital services in all public hospitals in the Hong Kong SAR. It is an independent organization which is accountable to the Hong Kong Government through the Secretary for Food & Health. It took over the management of the 38 public hospitals and institutions and a staff of 37,000 on 1 December 1991. Currently, the HA manages 41 public hospitals and institutions, 48 specialist outpatient clinics and 75 general outpatient clinics. As at 6 June 2008, it employed approximately 53,000 staff.

1.5 Management of health care services is undertaken by the Head Office (hereinafter referred to as "HAHO") directorate under the HA Chief Executive (hereinafter referred to as "the HA Chief Executive") through to the hospitals by way of regional Clusters (or groups of hospitals) in 7 regional areas. Each hospital is located within a regional Cluster headed by a Cluster Chief Executive. There is a management team in each hospital headed by a Hospital Chief Executive. The following chart illustrates the organisational structure of the HA :

Organisational Structure of the HA



Details of the abbreviations of the hospitals are found at **Annex I.**

Circumstances Leading to the Inspection

1.6 In March 2008, a complaint was received by the Commissioner's Office that a patient's data had been misplaced as a result of the loss by an employee of the United Christian Hospital of a Universal Serial Bus (USB) flash drive (hereinafter referred to as "USB drive") containing the complainant's personal data.

1.7 On 26 April 2008, the loss of patients' data in the United Christian Hospital mentioned in paragraph 1.6 above was reported by the media.

1.8 On 5 May 2008, the HA Chief Executive announced that there had been nine incidents (including the incident mentioned in paragraph 1.6 above) of loss of patients' data in the preceding 12 months in five hospitals[1]. The number of patients involved was approximately 6,000.

1.9 Also, on 5 May 2008, the Commissioner's Office was notified by telephone from the Prince of Wales Hospital that a USB drive containing the personal data of about 10,000 patients had been lost. The 10 incidents of loss of portable electronic storage devices in the last 12 months involved the loss of personal data of some 16,000 patients.

1.10 The series of incidents suggested inadequacies in the personal data system managed by the HA. Given the sensitive nature of the patients' data, the significant number of individuals affected and the substantial amount of patients' data involved, the Commissioner considered it was in the public interest that the whole system should be examined. In order to allay public concern, effective procedures should be put in place to prevent any recurrence and to restore public confidence in the HA's ability to keep secure personal data that had been provided to it by patients receiving medical services.

1.11 The Commissioner resolved that a three-pronged approach should be made to ascertain the scale of the problem and to enable him to make recommendations to prevent further recurrence. Accordingly, he decided to:

(a) proceed with the investigation under section 38(a) of the Ordinance in respect of the complaint received in relation to the loss of patients' data by the United Christian Hospital;

(b) proceed with a self-initiated investigation under section 38(b) of the Ordinance of the nine cases of loss of patients' data reported by the HA Chief Executive and notified to the Commissioner's Office under paragraphs 1.8 and 1.9 above in respect of those hospitals where losses had occurred and no complaints were received; and

(c) instigate an Inspection of the HA's personal data system under section 36 of the Ordinance in relation to the security of patients' data with a

[1] Namely, Pamela Youde Nethersole Eastern Hospital (4 cases), Tuen Mun Hospital (1 case), Kowloon Hospital (2 cases), United Christian Hospital (1 case, i.e. the case mentioned in paragraph 1.6), Sai Ying Pun Jockey Club General Outpatient Clinic (1 case).

view to making recommendations to the HA to promote compliance with the data protection principles of the Ordinance, in particular, DPP 4 .

1.12 The purpose of the Inspection was to examine the adequacy of the personal data system used by the HA by enquiring how such system for protecting and keeping secure the personal data of patients was effectively implemented via the Clusters to the hospitals managed by the HA. Due to financial and resource constraints, the Commissioner was constrained to limit the Inspection of the HA's personal data system to that implemented by one hospital as an example of all the hospitals managed by the HA.

1.13 The Commissioner chose The Ruttonjee Hospital and Tang Shiu Kin Hospital (which are hereinafter referred to as "the Hospital") for the Inspection for a variety of reasons. These included the fact that the Hospital is of average size and is not one of those undergoing investigations by the Commissioner. There were the additional advantages that the Hospital had until 1998 consisted of two separate hospitals both having a long established history of health care within the community. The larger of the two, the Ruttonjee Hospital, began its existence as a naval hospital in 1842 (on the western side of the hill at Wanchai Road, there stands a gate which at one time gave access to a quay on which sailors were carried directly to the Hospital from the harbour). For many years, it was known as the Ruttonjee Sanatorium managed by the Hong Kong Tuberculosis, Chest and Heart Diseases Association until 1991 when it was taken over by the HA. It has some 572 acute and general beds in different specialties and provides a 24-hour Accident & Emergency service. The Tang Shiu Kin Hospital was established in 1969 to replace the Eastern Public Dispensary and was named after its benefactor, the late Sir Tang Shiu Kin. Its Accident & Emergency Department was relocated to the Ruttonjee Hospital in September 2002 and the hospital is now a Community Ambulatory Care Centre. The combined hospitals were thought to provide a practical example of the management by the HA and in particular the personal data systems in operation some years after their consolidation. The Hospital belongs to the Hong Kong East Cluster of Hospitals (hereinafter referred to as "HKEC") and is accountable to the Cluster Chief Executive and ultimately to the HA Chief Executive.

1.14 On 8 May 2008, the Commissioner served on the HA a notice under section 41 of the Ordinance that he intended to carry out an Inspection pursuant to section 36 of the Ordinance of the personal data system operated by the HA in relation to the handling of patients' personal data with a view to making

recommendations to promote compliance with the Ordinance and in particular, DPP 4.

1.15 On 9 May 2008, the Commissioner led his staff to a meeting he had requested with the HA Chief Executive. The purpose of the meeting was to raise privacy concerns over the repeated recent occurrences of data loss and in particular, the loss of USB drives containing the data of a substantial number of patients. The HA Chief Executive briefed the Commissioner on the immediate action that had been taken to tackle the security risks in using portable electronic storage devices to store patients' data including restriction of staff-owned portable electronic storage devices to store such data and the steps taken to notify the parties affected by the losses. The Commissioner informed the HA Chief Executive that he had exercised his power to investigate the various cases of reported losses of patients' data and that he also intended to carry out an Inspection of the personal data system of the HA and would, if appropriate, make recommendations on measures to protect patients' data for consideration by the HA. The Commissioner informed the HA Chief Executive that he would inspect the HA's personal data system through the Tang Shiu Kin Hospital as well as (at the suggestion of the HA Chief Executive) the Rutonjee Hospital. The HA Chief Executive gave an assurance that he and the staff of the HA and the Hospital would fully co-operate in the Inspection. At the Commissioner's request, the HA Chief Executive also agreed to provide him with all relevant policy and practice documents relating to patients' data security promulgated by the HA, the Clusters and the Hospital. At the suggestion of the HA Chief Executive, the Commissioner agreed that he and his team would make a pre-Inspection visit to the Hospital during the week ended 16th May 2008 to gain an initial understanding of the HA's personal data system, its computer systems and the working environment as implemented by the Hospital.

Scope of the Inspection

1.16 The intention of the Inspection was to focus on the following:

(a) patients' data collected by the HA; in particular

(b) the storage and handling of patients' data in electronic form; and

(c) the adequacy of the security safeguards promulgated by the HA to protect patients' data collected by the hospitals under its management in compliance with DPP 4.

The Inspection Team

1.17 The Inspection team (hereinafter referred to as "the Team") was led by the Commissioner, Mr. Roderick B. Woo and assisted by the Deputy Commissioner, Mrs. Bonnie Smith. The Team was made up of officers from the Compliance Division, the Operations Division and the Legal Division of the Commissioner's Office as well as four consultants (hereinafter referred to as "the Consultants"). A full list of the members of the Team is at **Annex II.** The Consultants were invited by the Commissioner because of their expertise in the medical, information technology, privacy and legal fields. They were asked to assist the Commissioner, among other things, in forming a balanced view and making constructive and useful recommendations to the HA.

CHAPTER TWO

Chronology of Events

2.1 The Ordinance does not prescribe the methodology for an inspection to be carried out under section 36 of the Ordinance. In carrying out the Inspection, the Team refers to the statutory requirements to be complied by a data user under the Ordinance. In order to assess the level of compliance with DPP 4 in respect of the security measures adopted by the HA to protect patients' data, the Team had examined the policies and practices of the HA, conducted on-site inspection of the data security system of the HA as implemented by the Hospital, interviewed officers of the Hospital and the HA who were responsible for IT security, training and education, supervision of compliance and privacy audit. Questionnaires were also designed and randomly selected staff of the Hospital were interviewed to gauge the staff's level of privacy awareness.

2.2 At the meeting on 9 May 2008 (paragraph 1.15), the Commissioner asked for and the HA agreed to provide the Team with documentation in respect of the manuals, guidelines and practices on its data protection policies and its organization at Head Office, Cluster and hospital levels. A very substantial volume of documentation was made available and included the following:

(a) *Manual on Personal Data (Privacy) Ordinance* (Revised edition December 1996);

(b) *Clinical Data Policy Manual* (v. 0609, published Sept. 2006 and last modified May 2008);

(c) *Manual of Good Practices in Medical Records Management* (January 2001);

(d) *Information Security Policy & Procedure Manual* (Revised May 2008);

(e) *A Practical Guide to IT Security for Everyone Working in Hospital Authority* (May 2008);

(f) *Electronic Communications Policy* (v. 1.0 January 2005);

(g) *Notice on Application for Access to Electronic Clinical Data at Corporate Level by HA Staff;*

(h) *A draft Paper on Disclosure of Patients' Information* (May 1999);

(i) HAHO Information Technology Circular No. 1/2008 *Enhanced Measures on Enforcing Personal Data Security* (Issued 14 May 2008) (hereinafter referred to as "the IT Circular");

(j) HAHO Operation Circular No. 9/2008 *Policy on the Management of Loss of Electronic Devices Concerning Patient Identifiable Personal Data* (issued 18 May 2008)*; and*

(k) HAHO *Code of Conduct*.

2.3 The Team met frequently from the outset and spent a considerable amount of time in sifting through the documentation produced by the HA, assimilating the numerous policy documents, guidelines and statements of practice in order to fully acquaint themselves with the operation of the HA personal data security system. The Team assessed the relevance of the documentation received either by way of documents provided by the HA or through conversations with senior staff of the Hospital. Check lists were prepared by the Team for use in the Inspection.

2.4 At the suggestion of the HA, in the afternoon of 16 May 2008, the Team visited the Hospital and met with the Hospital's senior management (including the Hospital Chief Executive) and several representatives from the HAHO for a pre-Inspection meeting. Following an agenda set by the Commissioner, the Team spent a number of hours listening to the explanation given of the manner in which the HA's personal data security system functioned in the Hospital. Members of the Team were taken to different areas of the Hospital in order to familiarize themselves with the on-site operation of the Hospital's systems. A number of points of clarification were sought from and given by the staff of the Hospital. During the course of discussions, the Commissioner requested the senior staff of the Hospital to make a submission to him of the HA's data protection policies and practices as applied in the Hospital.

2.5 Following the initial visit to the Hospital, the Team discussed at length and designed a questionnaire to be completed by staff of the Hospital during the Inspection. The purpose of the questionnaire was to ascertain the level of awareness by the staff of the HA's policies in relation to data security, how these policies were applied by medical staff working within the Hospital and to what extent areas of concern had been identified by the staff and how far they had complied not only with the HA's policies but also with DPP 4.

2.6 On 20 May 2008, the Hospital made the submission requested by the Commissioner entitled "*Our initiatives in Protecting Patient Data Privacy in Ruttonjee & Tang Shiu Kin Hospitals, Hong Kong East Cluster, Hospital Authority*".

2.7 On 21 May 2008, the Hospital's Data Controller was interviewed by the officers of the Commissioner at the Hospital.

2.8 The Inspection of the HA's personal data system as implemented by the Hospital took place on Friday 23 May 2008 and continued on Monday 26 May 2008.

2.9 During the Inspection on 23 May 2008, about 100 randomly selected staff were interviewed by the officers of the Commissioner's Office to answer the questions set out in the questionnaire. An appeal to all staff of the Hospital to send in opinions on the HA's personal data system direct to the Commissioner's Office was made on the Hospital's Intranet on 27 May 2008.

2.10 Follow-up questions were raised and clarifications sought from the HA and the Hospital by way of written and verbal communications between 26 May 2008 and the writing of this Report.

2.11 On 12 June 2008, the Team met the HA Chief Executive and his staff to clarify a number of outstanding issues arising from the Inspection. Likely recommendations at that time were made known to the HA which was given the opportunity to respond to the same. The draft Inspection Report was also sent to the HA on 18 June 2008 for verification of the facts mentioned therein. The HA's responses and comments were carefully considered and where appropriate have been incorporated in the final Report.

The meeting held on 12 June 2008 attended by the HA Chief Executive, Mr. Shane Solomon and the Commissioner together with members of the Team.

CHAPTER THREE

The Personal Data System of the HA

Personal Data held by the HA

3.1 Three broad categories of personal data are held by the HA[2]:

(a) Personnel records which include personal details, job particulars, details of wages, payments, benefits, training, qualifications, disciplinary matters and performance assessment;

(b) Medical records which include records containing information relating to the physical and /or mental health of individual patients;

(c) Other records which include award of contracts, scholarships, appointments to the HA Board and Hospital Governing Committees of hospitals, administration files, flimsy files, public complaints, personality profiles; etc;

For the purpose of the Inspection, the Team was only concerned with patients' medical records.

Patients' Data

3.2 The *Clinical Data Policy Manual* (hereinafter referred to as "the Manual") of the HA defines "patient" as any person who is receiving/has received services from the HA.

3.3 **Section 2** of the Ordinance defines "**personal data**" as *"any data:*

(a) relating directly or indirectly to a living individual;

[2] Section D of the *Manual on Personal Data (Privacy) Ordinance* of the HA

(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."

3.4 According to the definitions given by the HA in its various manuals and guidelines, "patients' data" is taken to mean data of the patients that are collected in the process of clinical care, including demographic, administrative and clinical data, whether or not they are stored electronically (for example in the Clinical Management System (hereinafter referred to as "CMS")) or in a hard copy. The term "clinical data" was in turn defined by the HA to mean personal data that are related to the physical or mental health of an individual and/or the health care that the individual receives.

3.5 Patients' data in the form of medical records may be in hard copy, electronic or photographic (such as X-rays) form. The Team was told that in the Hospital, 66% of all transactions were recorded electronically and the remainder on paper.

3.6 Insofar as patients are living individuals and their data collected by the HA are recorded in a form rendering it practicable for their identities to be directly or indirectly ascertained, the data fulfill the definition of "personal data" under the Ordinance.

The HA's Patients' Data System

3.7 The HA's personal data system for the handling of patients' data is considered one of the largest in the Hong Kong SAR with three million transactions logged every day. The HA's clinical IT systems for handling patients' data were developed in-house by the HA's IT Department with the involvement of users, i.e. doctors, nurses, allied health professional representatives and have been implemented in the public hospitals managed by the HA.

3.8 The Team found there are two major clinical IT systems. One is a local area network based system (CMS) whilst the other is the web based electronic patients record system. Other departments such as the laboratory and the pharmacy have their own systems which feed into the two main systems

referred to above. Most of the workstations are "closed" stations with the USB ports disabled and only Intranet communications are permitted. Paper records of patients' data are stored in the Medical Records Store of the Hospital when they are not in use.

3.9 The Team was told that the extent of access to patients' data is defined according to the staff's grades and roles. It is governed by two principles namely, **Patient under Care** and **Organizational Need to Know**. Other than in accordance with these two principles, access to patient data is strictly prohibited by the HA. This prohibition is reiterated in a number of documents and policy manuals promulgated by the HA.

3.10 According to the Manual, where health-care professionals are involved in the care of a patient, they have a right of access under the principle known as "Patient under Care" to access clinical data relevant to the care of that patient. "Organizational Need to Know" is broadly defined under the Manual to mean access to patients' data required other than for patient care, e.g. for clinical audit, for clinical research and teaching purpose, for management audit and internal investigations, etc.

3.11 Application for CMS user account for access to a patient's data can be made by two means, (i) on-line; and (ii) paper form. The applicant is required to indicate on the application form that he satisfies one of the two principles referred to above.

3.12 In effecting compliance with the requirement that one of the principles must be satisfied before access is given to patients' data, the documentation discloses that the HA has adopted a zoning system for audit controls to prevent abuse of the system. Section 3.3 of the Manual describes three zones of audit controls, namely, Red, Amber and Green representing different levels of security risks for access to patients' data. The "Green Zone" means *"access to patients' data which is supported by face-to-face patient contact or is within a reasonable period of the patient's attendance or admission"*. The Team was told that for the purpose of facilitating the HA's IT Department to develop the appropriate programme, in practice the "reasonable period" is initially set at 365 days before or after attendance. However, this is not reflected in the Manual. The Green zone is regarded as the lowest level of security risks. Contrastingly, the "Red Zone", which includes access to hospital employees' data, is the highest level of risk and applies if neither of the two principles referred to in paragraph 3.9 above is satisfied. The Manual recommends that

audit of Red Zone applications should be carried out every month and that there should be an alert mechanism whenever an application is made for Red Zone access. The "Amber Zone" is loosely defined in the documentation as meaning *"access to patient data which is not covered by the Green or Red Zones*". However, as seen in paragraph 3.24 below, the documentation of the zones does not match reality. The HA claimed that this was because the implementation of the three zone concept was being progressively implemented to minimize disruption to patient care. It expected full implementation in 2008. The Team, however, did not find any express statement of policy to support this claim.

3.13 On commencing work with the HA, all staff are required to sign an undertaking to comply with the Ordinance and to observe patient confidentiality. According to the *Notice on Application for Access to Electronic Clinical Data at Corporate Level by HA Staff* issued by the HA, anyone who wishes to access electronic clinical data residing in the HA clinical systems at corporate level must complete an application form stating the reasons for wanting access and the period when that access is required. Support from the applicant's supervisor as well as from the HA's subject officer is required. Application forms for CMS User ID and CDARS[3] User have been devised by individual hospitals and take different forms. However, the HAHO expects all hospitals to adopt the requirements stipulated in "Notice on Application for Access to Electronic Clinical Data at Corporate Level by HA Staff".

Data Security Governance

3.14 The HAHO oversees all governance issues on data security and develops policies, guidelines and instructions relating to the collection, use and security of patients' data. At the Cluster levels, different committees have been formed to deal with specific matters falling within their respective purviews.

3.15 In October 2006, the HKEC under the HA set up a Cluster Data Privacy Committee (hereinafter referred to as "CDPC") to manage privacy and security issues. The scope of the Committee's work was *"to formulate and monitor the implementation of policies and guidelines for data privacy and security in*

[3] Meaning Clinical Data Analysis and Reporting System, which relates to the conduct of medical research.

HKEC in the following areas according to the HA's Clinical Data Policy, other related polices and relevant ordinances : (i) managing access controls, (ii) approving requests for data access, (iii) conducting access audits, and (iv) investigating possible breaches". The terms of reference of the CDPC are at **Annex III**. It appears logical to the Team that request for data access by hospital staff falls within the purview of the CDPC. However, the HA confirmed that requests for data access by hospital staff are processed by the Hospital IT Development Committee (hereinafter referred to as "the IT Committee"). In practice, the CDPC handles appeals against decisions made by the IT Committee.

3.16 A Cluster IT Steering Committee was set up in 2000 and oversees all matters related to data protection as part of its monitoring of the IT issues in the Cluster. The HA explained that after the establishment of CDPC in 2006, the monitoring and policy setting roles have been passed to the CDPC.

3.17 A Cluster Ethics Committee (hereinafter referred to as "CEC") was set up in 2000 and its scope covers, *inter alia*, both clinical and research ethics and the provision of recommendations related to the use of identifiable patients' data in research and studies. Its terms of reference are at **Annex IV.**

3.18 A Cluster Medical Records Committee was also set up in 2008 to develop, review and update Cluster policies, strategies, standards and work processes for medical record services amongst Cluster hospitals.

3.19 At hospital level, the IT Committee has been in existence since 1996 and focuses on patients' privacy issues at its half-yearly meetings. The Team was advised that this Committee also processes requests for access to patients' data made by the staff of the Hospital and CDPC acts as the appeal body.

3.20 The security of patient data is one of the review items included in the Hospital's Annual Plan (Section 3: Standard 53). This requires all the HA managed hospitals to conduct self-assessments to ensure that there are guidelines on the security and confidentiality of medical records and health information and access to patients' clinical data. Missing records are indexed and reported to the Hospital management after a thorough search. The HA further elaborated to the Commissioner that the hospitals are required to report results of the self-assessments to its Hospital Governing Committee and to the HAHO and that compliance with Section 3 Standards is subject to corporate audit following a risk-based assessment. No evidence has been provided by

the HA to show that there currently exists a principled and systematic audit of privacy risk applied by the HAHO to all hospitals.

3.21 A half yearly audit on compliance with data protection principles is conducted by the Hospital. The last audit of the Hospital was conducted on 25 September 2007.

3.22 An annual audit is also conducted by the Hospital on open CMS workstations by its own IT Technical Support Team[4] to ensure that access to CMS is password controlled and that the auto log-out function is available. This is done in the Hospital on the initiative of the Hospital management.

3.23 The Hospital has also developed its own Patients' Data Privacy Checklist distributed to departments annually for completion. The findings are reviewed by the Hospital management for quality improvement. The HA explained that this checklist has also been shared with other hospitals through the HA's networking arrangements. There was, however, no stated policy and practice to show that this is a prescribed process to be followed by all hospitals under the HA's management.

3.24 The Manual provides for a Red, Amber and Green Zones as described in paragraph 3.12 above. The Red Zone does not exist. According to information provided by the HA, it could not be implemented because it involved the automatic matching of the personal data of the HA's staff with the patients' data collected under CMS in order to ascertain which staff-patient's data had been accessed without authority. Such matching might contravene the Ordinance as the personal data of the HA's staff had been collected and kept for HR purposes and should not be used for other unrelated purposes, such as matching their data collected for medical care purposes. Consequently, the Red Zone was not put in use. In addition, the Amber Zone was not implemented as documented. So in practice there are only the Green and Non-Green Zones. The Green Zone is usually much broader than "Patient under Care" for most HA staff since Green Zone access covers not only for any patient who is being cared for but also where access is made within the period of 365 days before or after attendance of the patient.

[4] According to information supplied by the Hospital, it has three IT staff, including one Computer Operator, one Technical Services Assistant and one General Service Assistant, headed by a Hospital Manager. The audit is carried out by a team of three composing of the Hospital Manager, the Computer Operator and one professional medical officer.

3.25 In the absence of a Red Zone or a correctly implemented Amber Zone, any audits were re-classified as covering the Non-Green Zone and were carried out by studying the pattern of audit trail logs. The significance of "audit trails" was explained in clause 3.3 of the Manual which states that *"all access to patients' data are logged. The audit trails may become evidence in legal proceedings and thus should be prevented from deletion, overwriting or modification. The audit trails are retained as long as the patient record exists."*. The Hospital confirmed having performed at least 15 audits on the proper use of CMS between 2001 and 2006 by randomly selecting up to 5% of the staff's audit trail logs recorded in the computer system for analysis. After formation of the CDPC in 2006 which resolved to set up guidelines and criteria to standardise the audit, there had only been one audit of the audit trail logs which took place in May 2008.

3.26 The HA's disciplinary policy and procedure state that unauthorized access by any staff to confidential or restricted information relating to patients, including patients' records can amount to gross misconduct for which disciplinary action may be taken. This may result in, depending on the circumstance of each individual case, the issue of a warning, suspension from office, dismissal or any other action as may be appropriate.

Staff Training

3.27 On commencing work with the HA, all new staff are required to attend an orientation programme which includes a course on data privacy. The Hospital has organized several fora and on three occasions between 2005 and 2008 has invited officers of the Commissioner's Office to address staff on data privacy issues. The HA confirmed that the importance of data privacy has been promulgated through various means including through the Cluster newsletter, *Eastlink*, FAQ on the Intranet, etc.

CHAPTER FOUR

The Inspection

Preliminary

4.1 Following internal discussions and a study of the documentation provided by the HA together with the assistance of the Hospital management, the Commissioner decided that the Inspection should concentrate on the following main areas within the HA's personal data system as implemented by the Hospital:

(a) The HA's policies and practices related to the security of patients' data;

(b) The adequacy of the security of the HA's Information Technology System;

(c) The supervision, training and education of the HA's staff in handling patients' data security; and

(d) The systems of audit of patients' data security and the containment plan in the event of a security breach.

4.2 A pre-Inspection meeting with the senior management of the Hospital and relevant subject officers from the HAHO took place on 16 May 2008 during which the on-site operation of the data security system of the Hospital was shown to the members of the Team (see paragraph 2.4).

21 May 2008 : Interview with the Hospital's Data Controller[5]

4.3 The Hospital's Data Controller, who has other duties apart from being the Data Controller, was interviewed at the Hospital on 21 May 2008. During the course of the interview, he was asked for a copy of his list of duties but indicated that he did not have a formal or single list. He had been appointed by the Hospital in 2002 to carry out, in addition to his main duties, the duties

[5] Under the *Manual on Personal Data (Privacy) Ordinance*, this is the person nominated by each hospital to ensure compliance with the Ordinance.

of Data Controller. He said that there was no special pre-requisite skill required of a Data Controller. Data Controllers are usually experienced administrative staff but a few of them are medical doctors. He stated that his primary duty as a Data Controller was to handle and oversee the handling of data access requests made by data subjects[6] and the records in respect of which requests were made included staff records, patients' records and complainants' records. He is not required to report to the Data Controller of the HAHO. In response to the question whether the Data Controller would perform audit, he explained that he had to submit to the Cluster Chief Executive an audit checklist called "RHTSK Patient Data Privacy Checklist" once a year. The HAHO would carry out audit check on the Hospital and data protection is one of the issues being examined. He would also conduct regular visits to data collection centres and other data work stations at random.

4.4 On training, he said that the Cluster HR would organize orientation classes a few times each year for new staff during the course of which some training on the management of personal data was included. Seminars on data protection had been organized by the Cluster in recent years. He said it is not his responsibility for ensuring that training on personal data protection is given to the staff in the Hospital but he would help or participate in these activities as required.

4.5 In relation to the dissemination of information on data protection, he said that relevant policies & guidelines from both HAHO and the Cluster were e-mailed to relevant staff by the Hospital management and hard copies provided to those staff with no access to a computer work station. Updates on data protection would be provided by the Hospital management and these would be localized in order to make them more relevant to the Hospital but such updates have to meet the core requirements of the HA's guidance.

23 May 2008 and 26 May 2008 : the on-site Inspection

4.6 The Team invited the representatives from the HAHO and the Hospital to give presentations on the different aspects of handling patients' data security (see sub-headings below) to be followed by question-and-answer sessions where

[6] A data subject has the right to make data access request to the data user under section 18 of the Ordinance.

questions were freely asked by members of the Team to obtain further details, explanations or elaborations from the Hospital. This format was followed throughout the Inspection exercise. A walk-through of the various departments of the Hospital led by the Hospital management was also conducted.

Inspection of the security policies and practices

4.7 During this session, the Hospital representatives demonstrated to the Team the functional roles played by the various committees at the Hospital and Cluster levels that oversee data privacy. The hospital committees have jurisdiction limited to the hospitals whereas the Cluster committees oversee all the matters under their purview in the Cluster hospitals. The Cluster CMS Working Group focuses on management of clinical electronic data contained in the CMS. The CDPC pays attention to the privacy issues of both electronic and paper based patients' data. The Cluster Medical Records Committee oversees all the management issues related to patients' clinical records with special attention to paper records. The CEC deals mainly with clinical research applications. Applicants for research are reminded to follow strictly the ethics of data privacy.

4.8 The Cluster committees compose of staff from various hospitals, sometimes with common membership.

4.9 The Hospital representative informed the Team that the Hospital Data Controller's main job duties are to handle administrative works and he was appointed as Data Controller in addition to those main duties. He was not a member of either the CEC or the CDPC. The Team enquired about the Data Controller's job description and it was subsequently referred to the Operations Circular No. 13/2007 on *Compliance with HA-Related Ordinances* which contains lists of responsible officers. Besides, the *Manual on Personal Data (Privacy) Ordinance* stipulates that a data controller is nominated by each hospital to ensure compliance with the Ordinance by that hospital. Save for the mentioning of the general duty to *"ensure compliance with the Ordinance"*, there are no documents prescribing the specific functions and roles to be played by the Data Controller.

4.10 The Team was led through a typical application for access to a patient's data for research purposes under the control of the CEC. An application form has

to be completed with all necessary details and a declaration made as to the reasons for the application before it is submitted to the Secretariat of the CEC. The application is given to the chairman of the CEC who can give expedited approval himself if there is no clinical or privacy risk in terms of sensitive data being included (albeit that the use of HKID numbers is not included in any such risk assessment). If he has reservations, he may refer the matter back to the applicant for more information or submit it to the CEC for full committee approval. A standard CDARS User Application Form was produced for the Team's inspection.

4.11 The next area of control demonstrated by the Hospital representative was that of the CDPC which in addition to determining access to Red Zone data, also approves any general upgrading of the level of access to patients data, including access to Red Zone data and access to patients' data together with their HKID numbers. Decisions of the CDPC are based on a directive from the HAHO and any special situations relating to a particular hospital. Exceptional requests are handled by the CDPC on a case-by-case basis and are endorsed retrospectively by the Cluster Management. Upon request from the Team, the Hospital agreed to provide copies of the minutes of meetings of the CDPC[7].

4.12 The Hospital representative then addressed an area which gave rise to the original complaint against United Christian Hospital, namely, the loss of data on a removable electronic storage device. Members of the Team were referred to the IT Circular issued by the HA on 14 May 2008 following the reports of data loss from a number of hospitals managed by the HA. The IT Circular gives clear instructions on the use and security of USB drives for downloading data including a requirement that the USB drives so used must support encryption and password lockdown features and shall be centrally supplied by the HA.

4.13 Following the issue of the IT Circular, staff members are required to seek approval for any downloading of patients' data from Cluster management. The IT Circular indicates that downloading of patients' data is not allowed unless "*absolutely necessary for patient care*". Data may only be downloaded in accordance with the IT Circular, with Cluster management's consent and must be encrypted and password protected. The Team was shown *the User Application Form for Secure USB Flash Drive* which was recently devised

[7] The copies of Minutes of the three meetings held by the CDPC were subsequently supplied by the Hospital for the Team's inspection.

containing a declaration on IT security, confidentiality and copyright to be given by the applicant.

4.14 The Team was informed of the new policy issued on 15 May 2008 on "*Management of Loss of Electronic Devices Concerning Patient Identifiable Personal Data*"[8] that a systematic reporting system had been implemented and a duty to report imposed upon the staff, the supervisor, the department head and the hospital management respectively. A report is required to be submitted under the HA's Advanced Incident Reporting System (hereinafter referred to as "AIRS"). Remedial actions, such as reporting to the police, informing the patients and the Commissioner and issuing a press release are to be taken.

Questions and answers

4.15 When asked whether any risk assessment was undertaken by the CEC in processing expedited applications for access to patients' data for research purpose, the Hospital representative replied that consideration would be given to factors such as whether there was additional clinical intervention; whether there were sensitive privacy issues involved (for example, identified AIDS patients' data); whether there was involvement of vulnerable persons in the proposed study; and whether prior approval had been obtained from corresponding committees in other Clusters. The expedited approvals granted by the chairman of the CEC was not the subject of subsequent report and ratification by the CEC at meetings following the permission to access data. The Team raised concern at a certain overlapping of roles played by the CEC and the CDPC, e.g. in handling the access to patients' data containing identifying particulars.

4.16 The question was raised whether any guidelines existed to determine applications for granting levels of access to patients' data which currently appeared to be considered on a case-by-case basis. The Team was informed that the granting of access privilege is based on the two principles, namely, "Patients under Care" and "Organizational Need to Know" (see paragraph 3.9). For instance, a registered nurse is given access rights to those patients in the ward in which she works whereas a Departmental Operations Manager has access right to patients staying in all the wards within his / her department. On the other hand, staff with special duties such as Infection Control Team members and Patient Relation Officer will be granted access right to data of all patients treated in the Hospital on an "Organizational Need to Know" principle.

[8] HAHO Operation Circular No. 9/2008

Apart from the role-based approach, no prescribed guidelines for determining applications for access to patients' data were found to exist.

4.17 When the Team asked about the distinction between the levels of access to the Green Zone and the Red Zone, it was told that only retrospective vetting (at weekly intervals) is done of the Red Zone access. There would be an automatic audit alert when information which is required to be given in an application for access was not so provided. There was no reporting requirement to the HA although some hospitals chose to report to the HA. According to the Hospital, implementation of the Red Zone audit was discontinued in September 2007 when the HA received a reply from the Commissioner's Office on an enquiry raised about the matching of staff's record kept for HR purpose with staff-patient records kept under the CMS. Since the matching did not involve the taking of "adverse action" against the data subjects whose data were to be matched, it would not qualify as a "matching procedure" under the Ordinance for which application for approval by the Commissioner could be made. Fearing that such matching would contravene the other provisions of the Ordinance, the audit ceased and has not been revived.

4.18 Clarification was sought from the Hospital that no prior approval was required from the HAHO when the Hospital "localized" the HA's policies and practices by issuing its own circulars or internal guidelines in relation to handling of patients' data. The Hospital representative explained that these circulars and guidelines must not derogate from the HA's master policies and practices. The Hospital may however make minor variations if local circumstances make them desirable.

4.19 Certain inconsistencies and errors were noted by the Team in the application forms used by the hospitals[9] albeit that the basic intention was consistent.

4.20 When asked how the HA's policies and practices on data security were effectively communicated to the staff, the Hospital replied that the staff would generally refer to the *IT Security Manual* and *the Clinical Data Policy Manual,* which are available on the Intranet. Additionally, there are circulars and e-mails sent by the Hospital to the staff on a regular basis. The Team was provided with copies of circulars issued by the Hospital management

[9] e.g. the CMS User Application Forms, the CDARS User Application Forms and the IT Undertaking Forms. It appears that each hospital designs its own Application Form for CMS, the form may also be extended by some hospitals to cover other applications, such as CDARS and the the details of rules governing use as stated in the forms differ. Some typos were spotted in the User Application Form for Secure USB Flash Drive.

reminding staff of the duty to keep patients' data confidential and on the proper use of the CMS. According to further information supplied by the HA, it confirmed that the frontline staff will refer to the simple versions of the policies and practices[10], whereas the clinical management staff will refer to the full manuals and policies[11] and the IT staff will refer to the IT related manuals[12] for guidance in discharge of their job duties.

Inspection of the IT security system

4.21 A Power Point presentation was given by the representatives from the HAHO on the clinical systems of the HA which are summarized in the chart annexed at **Annex V.** The Corporate Clinical Systems are devised and have different sub-systems according to their own functions, for example, patient registration, patient treatment, X-ray examination and pathology test or pharmacy dispensing. Those persons carrying out those functions do not have access to any data other than what is necessary. There is a Wide Area Network linking the systems of the hospitals to the HAHO system.

4.22 When a staff member applies for a CMS user account, the application must be submitted via his or her management team. The system administrator will open a new user account by allotting a user ID and password for access. The staff member will be asked to fill in a user account application form and sign a confidentiality undertaking. Access to patients' data is given on a grade-based access control, e.g. the medical officer grade will be given access rights to data required by a clinician, such as prescription function and generic clinical request function. A nursing staff member on the other hand, will be given access rights to patients' data in relation to such matters as patients' discharge, bed assignment function, etc.

4.23 Whenever the CMS system is accessed, a key message reminding staff of the duty to keep patients' data confidential pops up. The system keeps transaction logs of all users, as to who they are, when, which and what history they access. These audit logs are used for investigation by hospitals, random checks and audit exercises.

---

[10] i.e. publications namely, "A Practical Guide to IT Security for Everyone Working in Hospital", "Protect Patient Confidentiality"; and "Frequently Asked Questions (FAQs) on Clinical Data Policy".

[11] i.e. "Clinical Data Policy Manual", "Manual on Personal Data (Privacy) Ordinance" and "Disclosure of Patient Information".

[12] i.e. "Information Security Policy and Procedure Manual" and the "Electronic Communications Policy".

4.24 The HAHO representative then gave a case study presentation on the security audit control implemented by the HA. The data were classified according to relative risks, from Red (i.e. high risk, e.g. staff record, patient of public interest); Amber (i.e. medium risk) to Green (i.e. low risk, e.g. patients' attendance). Implementation of the Red Zone audit was discontinued for the reasons set out in paragraph 4.17 above in September 2007. Attempts were made to use other methods for carrying out the audit but no effective solution was found. Hence, currently only a "Non-Green" Zone audit exists which is to be carried out based on audit trails and access reasons. However, the audit criteria have yet to be fully developed for identifying any abnormal trends of access. Disciplinary action may ensue[13] and depending on the severity of the violation ranges from counseling to issuance of a warning to reporting to the police. A Non-Green Zone audit was done by the Hospital in May 2008 based on the generation of a list of Non-Green Zone access trails for review and examination and according to the HA, the audit was based on commonly shared understanding among Clusters and on the professional judgment of the reviewer. The Team, however, expressed concern that the audit was not carried out on the basis of any stated audit methodology. The workflows of various departments of the Hospital were also presented to the Team to show how the systems are linked.

Questions and answers

4.25 When asked who was responsible for the IT security in relation to patients' data in the Hospital, the HAHO representative replied that it was the IT Committee. He added that of the 172 terminals in the Hospital, only 10 have active USB ports and the remainders are "closed" workstations with no access to a Windows operating system.

4.26 A query was raised as to the life span of the passwords used to access the system. The Team noted that while staff are regularly reminded of the need to change passwords, no expiry date is imposed on passwords. The Hospital representative explained that an attempt was made by the Hospital to enforce the change of passwords but this had resulted in chaos. The attempt has not been repeated. However, staff are required to change their passwords the first time the system is logged on after the account is opened. Staff are forbidden to

[13] According to the HA's Disciplinary Policy and Procedure, all employees are required to conform to HA rules and regulations established or promulgated from time to time. An employee who commits any breach of the HA rules and regulations is liable to the disciplinary procedures set out in the policy. The unauthorized access to confidential or restricted information related to patients, including patient records is regarded as act of gross misconduct.

share passwords with other users. The system does not enable the downloading or printing of the whole of a patient's records kept in the Hospital system.

4.27 On the question of using portable electronic storage devices for downloading patients' data, the HAHO representative replied that irrespective of the type of devices used (whether a notebook computer or a USB drive), the data must be encrypted to at least a 128 bit RC4 standard[14]. Following the HA's IT Circular regulating the use of portable electronic storage devices requiring approval for the use of such devices, staff are reminded to erase all patients' data contained in their self-owned devices. The Hospital staff are not required to use their own electronic storage devices for work but if they wish to do so, they must first register the device with the Hospital. There is no Wi-Fi system in the Hospital.

4.28 On the question of remote access to the HA's system, the HAHO representative replied that remote access cannot be made other than by a designated remote computer and data could not be downloaded from a workstation that has no capacity to do so (i.e. no access to a Windows operating system is installed). In relation to the use of electronic communications, the *Electronic Communications Policy* of the HA prescribes the rules for using e-mails, internet, etc. The sending of confidential data by e-mail though technically possible on computers with internet connections, is prohibited. Sensitive data concerning AIDS patients and those with psychiatric diseases are flagged and are separately maintained for added protection.

4.29 When asked whether live data of patients are used by IT contractors when testing the system, the HAHO representative replied that live data are not generally used. Instead, pseudo data are used and IT contractors were only allowed to work on-site and are required to sign a confidentiality undertaking. The HAHO representative was asked to provide the Team with the standard IT contract and the confidentiality undertaking for inspection[15].

4.30 A question was raised as to whether approval is needed to download patients' data including their HKID numbers for research purpose and whether the right of access automatically gives the user the right to download patients' data. The reply was that HKID numbers would not be included in any final research report so that it was immaterial that staff could access and download the numbers during the course of the research. The Team expressed concern that

[14] This standard as implemented in Microsoft Office is arguably not very secure.
[15] The documents were subsequently supplied by the HA.

this ignores the privacy risk of the data files. The HAHO representative also clarified that the application system has incorporated features of granting access right of individual application function (e.g. creation, enquiry, printing, data downloading, etc) for each staff. Therefore the system administrator can grant access right according to the rights and needs of the staff and it means that the right of access to patients' data does not automatically imply that he or she also gets the right to download the data.

4.31 In relation to the question of security features, the HAHO representative replied that the data downloading function has incorporated the features of password protection and data encryption. All staff having the right to download data must use the password protection and file encryption function when downloading data.

Inspection of the supervision of compliance, training and education given to staff

4.32 A presentation was given by the Hospital representative on the supervision of staff compliance with the data security policies and practices and the training and education given to staff on protection of privacy of patients' data.

4.33 The Hospital representative confirmed that circulars on maintaining patients' confidentiality and proper use of CMS were regularly issued and circulated to staff for information. Staff are required to sign and confirm that they have read the circulars. In relation to the proper conduct of electronic communications, an IT circular was issued by the HA on 19 January 2005 titled "*Electronic Communications Policy*" and on 14 May 2008, the IT Circular titled *"Enhanced Measures on Enforcing Personal Data Security"* was issued. Disciplinary action ranging from counseling, the issuance of a warning letter, dismissal or reporting to the police or law enforcement agencies will be taken upon discovery of improper access behaviour and gross misconduct. Staff are required to observe the HA's Code of Conduct which is provided to all staff as a handbook when joining the HA. Promulgation on protection of patients' data was also made through the Cluster Newsletter, the *EastLink* in February 2008.

4.34 Training programmes relating to personal data privacy are delivered by the HKEC HR to the staff of the hospitals, such as the Orientation Programme for Allied Health / Management and Administrative Staff (held once a year); Orientation Programme for Medical Staff (held twice a year), Orientation Programmes for Nursing Staff (held twice a year), Orientation Programmes for

Supporting Staff (held 3 to 4 times a year). Fora and Seminars on Personal Data Privacy were also held and officers from the Commissioner's Office had been invited to conduct seminars (three times between 2005 to 2008). The CDPC also held a forum on Access to Clinical Data and Clinical Data Policy on 13 December 2006 for the Cluster hospitals. From the statistics supplied by the Hospital, the attendance at these fora and seminars by staff was proportionately low. Commenting on this phenomenon, the HA claimed that this is a known issue in all hospitals due to shift work and the need to attend to patients. The HA expects those who do participate to play a planned role in cascading the knowledge gained to their fellow staff through team meetings, etc. However, no documentary policy or practice was produced by the HA to show the existence of the planned role.

4.35 The most recent Forum on "Personal Data Privacy" was one organized by the Hospital and the HAHO and was held on 20 May 2008 shortly after the Commissioner had served notice of the Inspection on the HA.

Questions and answers

4.36 A question was raised whether in relation to the shredding (of papers) service that was carried out by the HA's appointed contractor, there is proper supervision in place and whether there is monitoring of compliance with the required retention periods for the different types of data kept in the Medical Records Store. The Hospital representative replied that since storage space in the Medical Records Store is limited, there is every incentive on the part of the staff to destroy unnecessary data which are in paper form. The Team was requested to contact the HA for a copy of the standard service contract entered into with the shredding service contractor[16].

4.37 The Team was told that an audit was conducted by the Hospital once a year in ensuring the open workstations are password protected and there was proper auto log-out function.

4.38 The question was asked how the Hospital implemented the IT Circular on the use of USB drives. The Hospital representative replied that the Hospital would keep logs of such use and that any staff who needs to use a USB drive must apply for approval which was based on operational needs. Currently, there are 5 USB drives with encryption and password lockdown features allotted by the HAHO to the Hospital for its use. A registry of use was maintained in the HAHO.

[16] Copies of the service contract were subsequently supplied to the Commissioner for inspection.

4.39 A question was posed on how the large quantity of policies, information and materials that were made available on the Intranet were effectively communicated to the staff. The Hospital representative confirmed that more and more information was made available on the Cluster's Intranet, but he did not find that the staff had tended to check only information available at the Hospital level.

4.40 When asked whether there was a sharing of training materials amongst the Clusters, the Hospital representative replied that most of the training materials were prepared by a responsible officer at the HAHO and he noted that basically the same materials were used by all Clusters.

4.41 When asked whether staff members' level of knowledge of data security was reflected in the annual performance appraisal, the Hospital representative conceded that training on personal data privacy was not subject to as stringent a level of control as that on infectious diseases and occupational safety for which staff were compulsorily required to attend training and meet the required standard.

Inspection of the data security audit system and the containment plan in the event of data security breach

4.42 Presentations were given by the Hospital representative on the data security audit and containment plan. According to him, the Hospital's Annual Plan Section 3: Standard 53 was implemented some 10 years ago and hospitals are required to undertake self-assessment to ensure that there are guidelines on the security and confidentiality of medical records and health information and access to patients' clinical data. Missing records are required to be indexed and reported to the hospital management. Audit results are required to be reported to the Hospital Governing Committee and to the HAHO. The Hospital representative confirmed that the Hospital fully complied with the prescribed standards concerning patient data security and protection.

4.43 A half-yearly legislation audit on compliance with the Ordinance was also carried out, the last of which was done in September 2007. An annual IT audit was also conducted by the Hospital's own IT staff on password controls and automatic log-out functions. The Hospital recently devised a privacy checklist for use by the departments of the Hospital. The HA confirmed to the Team that the checklist has also been shared with other hospitals through the HA's networking arrangements.

4.44 The Hospital representative said that he had done about 15 audits of the audit trail logs between 2002 and 2006 when abnormal access to patients' data was found and analyzed by a random selection of up to 5% of the staff audit trail logs in the computer system. The audit work ceased since the end of 2006 as a result of the decision of the CDPC to take over the audit works and to devise systematic guidelines. However, the audit criteria were yet to be developed by the CDPC for systematic audit to be carried out.

4.45 The "Red Zone" audit was stopped for the reasons stated in paragraph 4.17.

4.46 As for containment plan, a system is now in place for reporting the loss of electronic storage devices containing patients' data through AIRS. The Operation Circular No. 9/2008 issued by the HA on 15 May 2008 sets out a reporting line. A staff member is required to notify his or her supervisor or the head of the department of any loss and submit a report through AIRS. A report is also to be made to the Police. The supervisor or head of department must also report the incident to the hospital Chief Executive and /or the Cluster Chief Executive who in turn will submit a report to the HAHO within 48 hours.

4.47 Upon the happening of an incident involving the loss of personal data which were stored in these electronic storage devices, the patients affected are to be informed. The Commissioner's Office shall also be informed and a press release prepared to report the incident.

Questions and comments

4.48 The Team was informed that audit by an examination of the audit trail logs is believed to be a sufficiently effective method. Members of the Team, while fully appreciating what had been done and achieved by the Hospital through the works of one of its medical officers, questioned the wisdom of over-reliance on the professional judgment of one person without principled methodology or objective criteria in place to follow.

4.49 The Team applauded the transparent steps taken by the HA to deal with data security breaches. The privacy loss caused to individuals was mitigated by the notification to them as soon as possible after the loss occurs. Proactive steps taken to notify the law enforcement authority and the Commissioner's Office are also encouraged as good practice.

The Walk Through

At Ruttonjee Hospital

4.50 Following the presentations and question-and-answer sessions, the Team was taken to inspect the Accident & Emergency Department, the Medical Records Store, the Pathology Department, a Medical Ward and the Physiotherapy Department of Ruttonjee Hospital in the afternoon of 23 May 2008.

4.51 During the course of the Inspection, members of the Team noted the following:

Accident & Emergency Department

(a) *Notices to Patients* in English & Chinese advising of the need for collection of personal data on registration are conspicuously displayed. A similar Notice is shown to patients when giving their personal data;

(b) Patients are required to present their HKID for verification;

(c) In the triage area, patients' medical records are temporarily placed in a tray covered with a green warning notice marked "Confidential" and states that *"According to the Personal Data (Privacy) Ordinance, unauthorized access to the information of this folder is in contravention of the law"*;

(d) All computer systems can only be connected to the Clinical Management System with no internet linkage;

(e) Trays containing patients' medical records in paper form are all covered with a green "Confidential" cover;

(f) Each patient is required to proceed to the counter for payment and registration when their assigned number is shown on a screen. Staff did call out patients by name for attending doctor consultations;

Medical Records Store

(g) All patients' medical records in paper form but excluding X-rays are stored in locked filing cabinets;

(h) Medical records of patients who have not attended the Hospital for more than 6 years are shredded on an annual basis and only unused non-

confidential paper is recycled. Shredding is carried out by a designated contractor appointed by the HA and is placed in sealed non-transparent plastic bags prior to weekly collection;

(i) Trolleys for transportation of medical records to and from the Store are covered with a tailor made cloth cover;

(j) Medico-legal medical data are stored in a separate locked room within the Store;

Pathology Department

(k) A file containing the blood types and HKID numbers of patients is downloaded to a stand-alone system once a month for main system down-time recovery purposes. The file is encrypted using a 128 bit RC4 encryption method. The stand-alone system is not linked to the internet;

A Medical Ward on the 9/F (designated "A9")

(l) All medical records and documents when not needed after rounds are collected and placed securely in trolleys in front of the nursing station;

Physiotherapy Department

(m) Staff mark the name, bed number and exercises to be performed on the patient's exercise card at each visit;

(n) The physiotherapist or a nursing staff marks the date and exercises performed on the patient's paper medical record immediately upon completion of the exercises.

At Tang Shiu Kin Hospital[17]

4.52 The Team then proceeded to inspect the following departments of the Tang Shiu Kin Hospital which does not provide in-patients service :

Registration and Payment Counter

(a) A similar Notice as those exhibited at the Ruttonjee was displayed at the reception desk;

(b) No computer systems have internet access;

(c) Each patient, on his first visit, would be given a card with his name and designated patient number (not HKID number) printed on it. He is required to bring back the card upon his next visit to the Hospital;

Medical Records Store

(d) All patients' medical data in paper form are securely locked in filing cabinets;

(e) Trolleys containing patients' medical data in paper forms are covered with a green "Confidential" cover;

(f) Only unused non-confidential documents are used as recycled paper;

(g) Unused confidential documents are placed in sealed non-transparent plastic bags and passed to the HA's designated contractor for shredding;

Exercise Room

(h) No computer systems situated in the open area have internet access;

(i) The auto log-out time has been changed from the usual 10 minutes to 1 minute as some of the computers' screens face the public areas;

[17] This is a separate block of building some distance away (about 10 minutes walking distance) from the Ruttonjee Hosptial's main building.

Family Medical Specialist Clinic

(j) A notice entitled "*Personal Information Collection Statement*" (in both Chinese and English versions) is displayed on the registration desk. A copy of such notice can be given to patients upon request;

(k) The workstations for access to CMS are not connected to the internet;

(l) Patients' medical records were all covered with the green "Confidential" cover;

(m) Each patient, upon his first visit, is issued a small medical record card entitled, "*Family Medicine Clinic / General Outpatient Medical Record"* with patient identification label containing his name, HKID number, sex and date of birth attached. On each visit, the medical officers and nursing staff mark the diagnosis and other medical details of the patient on the record card for the patient's own records and safe keeping.

The Commissioner and members of the Team were shown the CMS operation at the Accident & Emergency Department of the Hospital

Presentations given by the Hospital representatives to the Team on 23 May 2008

CHAPTER FIVE

The Questionnaire

5.1 The Team had the opportunity prior to the Inspection to review a substantial volume of documents provided by the HA dealing with the policies for the protection of patients' data, circulars that had been issued and committee minutes. As a result, it was possible from these documents and from the information provided in the meetings by the staff of the Hospital for the Team to identify those aspects of the HA's personal data system which justified further and more detailed enquiries in assessing the level of privacy awareness amongst the staff of the Hospital.

5.2 Face to face interviews with some 100 randomly selected staff of the Hospital were conducted on 23 May 2008 by officers of the Commissioner's Office. As the interviews were likely to cause some disruptions to the routine duties of the staff, advance notice was given to the Hospital of the event. The staff were shown a copy of the questionnaire in English but told that if they had difficulty in understanding any question, they would be provided with a Chinese version of the questionnaire. The disparity in results of some questions is explained by the fact that some staff members chose either to decline to answer a particular question or insisted on completing more than one response box[18]. A copy of the questionnaire and an analysis of the results of the questionnaire together with a summary of the suggestions for improvement referred to in paragraph 5.7 (o) below are at **Annex VI.**

5.3 Despite some responses which give rise to the concerns expressed above, the questionnaire provides no surprising conclusions. It has to be said that the Commissioner's officers were left with a feeling that there had been an element of assistance from the Hospital to its staff prior to the Inspection[19] in anticipation of the likely questions to be asked. There was some evidence to support this view including the responses to closer questioning of some staff

[18] See the Statistical summary of the answers made in some questions in the questionnaire in Appendix VI

[19] For instance, a Forum on Personal Data Privacy was held by the Hospital on 20 May 2008, immediately preceding the Inspection which is positively perceived by the Commissioner of having the beneficial effect of enhancing the privacy awareness of the staff by refreshing their knowledge and reminding them of the rules and regulations covered by the various manuals, policies and practices on protection of personal data privacy.

on certain questions which tended to indicate they had given a less than accurate response to the questions in the questionnaire. Whilst the responses are thought to be generally correct, the overall impression is that they should be treated with some circumspection.

5.4 That said, the open questions where opinions of staff were solicited are candid and show that the staff do think that more training is required to increase their level of privacy awareness.

5.5 Subsequent to the conduct of the questionnaire on 23 May 2008, a written appeal was sent to the staff of the Hospital to send in their opinions and comments on the security of patients' data to the Commissioner's Office direct. The Commissioner regrets to note that up till the writing of this Report, no written response has been received.

5.6 The particular areas of concern to the Team are set out below and reflect what they considered to be the more important aspects of the HA's policy on data security and the associated issues of retention, destruction, supervision, education and training.

5.7 The areas on which the Team wished to receive further information from users "at the sharp end" of the Hospital's data handling practices and the Team's comments following analysis of the completed questionnaires were as follows:

(a) Whether the Hospital's staff had received instructions on the requirement to seek prior approval before accessing a patient's data ? (Q.6)

A significant percentage (34%) said they had never received any such instruction. It appears that staff did not realize that obtaining a HA system password is the standard process for obtaining approval for accessing patients' data in the course of everyday work.

(b) Whether instruction had been given that access to patients' data can only be made if either of the two conditions of "Patient under Care" and "Organisational Need to Know" is satisfied ? (Q.8)

The high percentage of positive response (93%) was impressive.

(c) Whether staff log out after accessing data or whether they rely on the auto log-out after 10 minutes of inactivity on the work station ? (Q.10)

Reliance on the auto log-out (10%) should be discouraged.

(d) Whether staff share passwords to the system ? (Q. 11)

This is a malpractice (3%) and should be prohibited.

(e) Whether staff import patients' data and, if so, by what means? (Q. 12/13)

The responses are helpful in assessing work practices.

(f) Whether staff had downloaded or exported patients' data and, if so, whether it was password protected or encrypted ? (Q.14)

The use of encryption/passwords (83%) could partly be a result of the recent IT Circular issued by the HAHO.

(g) Whether authority was given for the downloading and, if so, by whom? (Q.15)

Nearly 20% apparently downloaded without authority. While this would clearly be a serious breach, the Team believes it is more likely to reflect a misunderstanding of the question as the Team accepts that the staff do require authority to download.

(h) Whether exported data were de-identified before export ? (Q.18)

An equal number of respondents (11 "yes" answers and 11 "no" answers) did not de-identify. There may well have been justification for not de-identifying and the Team took no issue on this. It was explained to the Team that this may be justified as it may be difficult to re-match CDARS data without retaining HKID numbers, but this still highlights the privacy risk.

(i) Whether staff are permitted to take patients' data outside the workplace and, if so, under what circumstances, for what reasons and on whose authority? (Q.27)

There might have been some confusion over the term "workplace" and the figures therefore may be misleading.

(j) Whether staff had stored patients' data on devices owned by them? (Q.29)

The high percentage of "no" response to questions (a) and (b) might be due to the recent issuance of the IT Circular prohibiting use of staff owned electronic storage devices.

(k) Whether staff are aware of the policies and guidelines issued to regulate the handling of patients' data and, if so, how clearly the policies etc were understood ? (Q.31)

The positive responses (98% to both parts of the question) are higher than was expected by the Team.

(l) Whether staff are aware of the policies or guidelines relating to notification of any loss of patients' data? (Q.34)

Similarly high responses.

(m) Whether staff had received any training on the security of patients' data and, if so, whether the training was adequate to enable them to understand? (Q.35/36)

The "Do not care" responses (3%) were disappointing.

(n) Whether staff are aware of particular problems within the Hospital, namely, the sharing of passwords, failure to log out after accessing data, widespread use of portable electronic devices and portable electronic devices containing data left unattended? (Q. 42)

The relatively high percentage of response on the issue that computers are not logged out after use corroborates what the Team saw in one department in the Hospital.

(o) Staff were also asked to comment generally as to how the existing personal data system of the Hospital could be improved so that patients' data could be better protected. (Q.44)

The observations were helpful to the Team in formulating recommendations.

CHAPTER SIX

Observations and Recommendations

Application of DPP 4

6.1 In carrying out the Inspection and in making recommendations to the HA, the Commissioner has to assess whether "all reasonably practicable steps" as required under DPP 4 had been taken by HA to protect patients' data. The measures to be taken by a health-care service provider to safeguard patients' data ought to be commensurate with the privacy risks associated with the collection, holding, processing and use of such data. Particular regard should be given to:

(a) the kind of data and the harm that could result if unauthorized access etc. should occur;

(b) the physical location where the data are stored;

(c) the security measures incorporated into any data storage equipment;

(d) the measures taken for ensuring the integrity, prudence and competence of those having access to the data; and

(e) the steps taken to ensure secure transmission of the data.

6.2 It has been the regulatory stance of the Commissioner that DPP 4 does not impose an absolute duty upon a data user to guarantee the security of personal data entrusted to it. DPP 4 only requires the data user to take such steps as are **"reasonably practicable"** to guard against unauthorized or accidental access, processing, erasure or other use of the data. The term "reasonably practicable" has appeared frequently within our jurisprudence over the years. The determining factors arising from those judgments[20] with which the Commissioner has been acquainted are that in order to demonstrate that reasonably practicable steps have been taken, it has to be shown that :

(a) there is an awareness of the risks (in this instance, of unauthorized or accidental access, processing or erasure of patients' data);

[20] Edwards v. National Coal Board [1949] 1 AER 743 and Marshall v. Gotham Co. Ltd. [1954] AC 360

(b) such risks have been identified; and

(c) a conscious decision or series of decisions have been made to balance, without gross disproportion, the steps that have been taken to protect that data against the "time, money or trouble" to be incurred in implementing them within the existing practices of the data user (in this instance, the HA and the Hospital).

6.3 In applying the test of what is "**reasonably practicable**" for the HA, the Commissioner is cognizant of the primary duty of a hospital which is to save lives and that duty is of paramount importance to the public it serves. A policy, guideline or manual that wholly prevents the incidence of human error has yet to be found. However, human error can be substantially reduced by the introduction of a better data security system and through proper supervision, training and education of the people who are entrusted with the handling of patients' data. A plea of "time, money or trouble" that is to be spent or incurred for taking these security measures cannot be readily accepted as justification or used as an excuse by the data user for delaying or avoiding the implementation of adequate security measures to protect personal data held by it. Given that the public hospitals system is administered by the HA, that a substantial number of patients is involved and a vast amount of sensitive data is handled and processed by it, the impact on patients' data security is critical. The overhaul of its patients' data security system will not only serve to restore public confidence but will also have a long term beneficial effect in the eventual implementation of the proposed e-Health platform. It is therefore much in the public interest that the HA adopts a high standard of security measures.

6.4 The Team acknowledges that important and significant efforts have been made by the HA to devise a patient data system that facilitates medical care while safeguarding data security. The general impression of the Team is that the HA has in place good and detailed policies and practice for protecting patients' data security, the standard of implementation and coordination of the policies and practice through the HAHO to the Clusters and the hospitals is only fair to satisfactory. However, more efforts are required in monitoring the compliance with the requirements of the Ordinance and the effective carrying out of systematic security audit in order to detect any early sign of data breach and non-compliance. Lastly, the staff's general level of privacy awareness shows the pressing need for improvement as many of the data breaches were committed as a result of human errors. To sum up, more efforts are required to

be taken by the HA in providing sufficient security protection to the storage and use of patients' data in electronic form.

6.5 The Inspection has enabled the Team to identify different areas of concern and to come up with corresponding recommendations to the HA to promote compliance with the security requirements of the Ordinance. In making these recommendations, the Commissioner is mindful that he should not dictate or assume the role of the management of the HA in deciding what is the best course of action to take. Like any other data users, this remains a decision to be exercised with the judgment of the HA. Hence, the recommendations, as they are, give flexibility for implementation which the HA may adapt to suit specific operational needs or circumstances in order to comply with the requirements of the Ordinance. These recommendations are set out below under different headings.

I Security Policies and Practices

Areas of concern:

6.6 There are voluminous and overlapping policy documents dealing with the handling of the security and the confidentiality of patients' data that make compliance by staff difficult. There is a lack of a regular systematic updating and reviewing process, e.g. *The PDPO manual on Personal Data (Privacy) Ordinance* was according to the HA, last updated in August 2007 by supplements and replacement made known on its Intranet; the *Paper on Disclosure of Patient's Information* is still in draft form with no definite date for its completion. There are several different manuals containing chapters or sections dealing with data stored in electronic form but no holistic and consistent approach for easy reference. It appears to be the tendency that for policies on handling paper records, the staff only refer to *The Manual of Good Practices in Medical Records Management* and for electronic data, they rely upon the simplified version of *The Practical Guide to IT Security* notwithstanding that there are relevant policies and guidelines that govern and regulate the handling of patients' data in either electronic or paper form. Revisions to the policies and practices are made in a piecemeal fashion.

6.7 Individual hospitals are permitted to "localize" the HA's policies and practices with no systematic monitoring by the HA to ensure that its policies are not

rendered less effective by such localization. There does not appear to be a regular compliance audit and monitoring to ensure that the various CMS User Application Form, the CDARS User Application Form and the IT Undertaking Form adopted by the hospitals comply with the HA's master policies and practices. .

6.8 The communication of the policies and resultant practices leaves room for improvement. The question remains as to how these voluminous policies, guidelines and practices can be effectively drawn to the attention of the busy medical staff. This is particularly so in relation to the security issues associated with the use of portable electronic storage devices. The circulars issued by the Hospital dealt mainly with "unauthorized access to patients' data" and "patients' confidentiality" without express reminders on the use and safe keeping of removable electronic storage devices[21].

Objective of the following recommendations:

The systematic formulation, review and updating of the data security policies and practices and their timely and effective communication to the staff.

RECOMMENDATIONS

1. To assign a HAHO committee / designated person with clearly defined terms and functions to devise, update, review and consolidate in a timely manner all manuals, policies and practices in relation to patients' data security.

2. The HAHO committee so assigned / designated person should also be charged with the function to lead, coordinate and monitor compliance with these policies and practices by all Clusters and hospitals, e.g. to devise standard CMS User Application Forms, the CDARS User Application Forms and the IT Undertaking Forms to be used by all hospitals.

3. At Cluster and hospital level, the Cluster Committees and Hospital Committees should be specifically charged with responsibilities for:

(i) Implementation of policies and procedures of the HAHO;

[21] It was only on 14 May 2008 that the HA issued the IT Circular on enforcing personal data security to all staff.

(ii) Reporting progress (and statistics) to the HAHO, where appropriate;
(iii) Identifying problems encountered in implementation; and
(iv) Recommending reviews to the HAHO to address the problems.

4. To consider and review all the existing manuals, policies, practices and documents to ensure that materials in relation to the handling of patients' data are kept up-to-date and to highlight the privacy risks associated with the use of patients' data stored in electronic form and their proper handling.

5. Where it is necessary for individual hospitals to "localize" the HA's master policies and practices to suit operational needs, they should continue to be subject to periodic and regular compliance audit by the HA to ensure that the localized polices and practices dovetail with the master policies and practices of the HA.

6. Steps shall be taken to facilitate the more effective dissemination of the security policies and practices to the staff so that they can have easy and quick reference (through accessible and transparent conduits, e.g. enquiring with the responsible officer or perusing relevant documents via the Intranet) to the correct points under the applicable policies and practices. In order to make the policies reader-friendly and to take into account the different ranks of staff and their job requirements, a layered notice approach may be developed by first, drawing the attention of all staff to the basic security requirements written in simple language and then linking them to the second level where specific rules and policies apply, e.g. items such as rules for using (i) portable electronic storage devices in the HA; (ii) making CMS user application or CDARS applications; (iii) taking patients' data outside the workplace for handling, etc.

II Cluster Committees and the Data Controller

Areas of concern:

6.9 The actual functions performed by the Cluster Committees sometimes overlap so that there might be confusion as to the respective roles played by these Committees in protecting patients' data privacy. For example, the CDPC was formed in 2006 and according to its terms of reference is responsible for data privacy and security issues, including managing access control and processing

request for data access and conducting access audits. In practice, however, application for access to patients' data for research purpose is processed by the CEC whose terms of reference do not contain any requirement for it to undertake any data privacy risk assessment before granting approval. The CDPC, since its formation, has not processed any application for increase of access privilege by users because in actual practice, the job is done by the IT Committee and the CDPC only handles appeals from decisions made by the IT Committee.

6.10 The IT Committee of the Hospital conducts its own audit trail logs reviews with no regular systematic policies and methodology in place. Those that were done were entirely a matter of judgment and decision by the hospital administration with no compulsory reporting requirements and follow-up action to be taken by the HAHO.

6.11 The role played by the Data Controller is vague. According to the interview conducted with the Hospital's Data Controller, he is primarily responsible for handling data access requests of patients and the yearly submission of privacy audit checklist on patients' data to the Cluster Chief Executive. No stated methodology is being used. He is not charged with clearly defined responsibilities for ensuring or arranging privacy training for staff nor does he sit as a member of the CDPC.

<u>Objective of the following recommendations</u>:

The functional roles to be played by the Cluster Committees be clearly defined and that of the Data Controller strengthened to protect patients' data security.

RECOMMENDATIONS

7. To review the roles to be played by the various Cluster and Hospital Committees so that there are clear terms of reference with no overlapping of functions. The processing of access to patients' data and the conducting of privacy audits should be clearly delegated under the purview of the relevant committees. In granting approval for access to patients' data, a privacy risk assessment by taking into account and balancing the different risk factors should be undertaken and documented. Common membership of key personnel may serve to ensure that there is co-ordination between committees.

8. To review and strengthen the role to be played by the Data Controller and to consider appointing him to sit as a member of the CDPC for effective functioning of his role.

9. To consider making it known to the staff that the Data Controller or such other designated person is one to whom enquiries on personal data protection matters should be made at hospital level.

10. For the sake of accountability and transparency, to consider appointing independent third parties as members of these Committees to participate in the decision-making process.

III Security Measures

Areas of concern:

6.12 While the Team recognizes the critical importance of accurate authentication of patients' identities in minimising medical errors, the unnecessary use of patients' HKID numbers for matching purposes other than authentication exposes the patients' data to avoidable privacy risk. It is found that patients' HKID numbers and demographic data are used on gummed labels and appointment slips which are bar-coded and which may not always be required for authentication. If it is necessary to verify the identity of the patient, this can be easily done by physical inspection of the patient's HKID number against the data kept by the HA through scanning the bar code. The HKID numbers of lists of patients are sometimes disclosed for research purpose to facilitate matching back to the patients' records and this raises privacy concern given that use of other less privacy intrusive alternatives, such as hospital numbers or patients' numbers can equally achieve the purpose.

6.13 It is noted that electronic data of patients outside the two main HA systems are kept for long periods without formal retention policies[22] that take into account the purposes of use involved and the privacy risk. For instance, electronic

[22] According to the HA, some data kept by the Laboratory and the Pharmacy Systems are purged regularly by following operational guidelines. There is, however, no systematic retention policy in place.

records of patients kept for administration, pharmacy and laboratory purposes should not be excessively retained. It is also noted that according to Clause 3.25 of the Manual, all access to a patient's data is logged and the audit trails are retained as long as the patient's record exists. Since the audit trails also contain patients' data which may be retained until the death of the patients, the retention period is excessive given that audit or review functions may already have been performed. The HA explained that in practice, the copy of audit trails extracted for audit will be deleted after the audit or review functions have been performed. The Team was concerned that the original audit trails are still held indefinitely.

6.14 The password control and automatic log-off mechanism presently used by the HA leave room for improvement given the absence of an enforced expiry date for the passwords.

6.15 Although the policies on use of portable electronic storage devices have now been implemented[23], they are insufficient to fully address other related and fundamental issues such as :

(i) reviewing the need for using such devices supported by valid reasons on a systematic basis;

(ii) the steps to be taken to continue "sanitization" of portable electronic storage devices;

(iii) the safe erasure of data contained in such devices when the purpose of their use is fulfilled;

(iv) the downloading of patients' data contained in documents intended to be used as templates;

(v) data created by the users of Microsoft Office which may contain patients' data, such as those used for writing medical notes and letters about patients which staff may bring home to continue to work on with their own personal computers, etc; and

(vi) the adequacy of the security protection in using the standard Microsoft Office encryption function when sensitive personal data, such as HKID numbers of patients are downloaded.

6.16 More steps should be taken to ensure the "integrity, prudence and competence"[24] of the contract IT staff who are charged with the responsibility of ensuring the IT security of the hospitals. For the standard *Contract for*

---

[23] IT Circular No. 1/2008 on "Enhanced Measures on Enforcing Personal Data Security".

[24] DPP 4 requires practicable steps be taken for ensuring the integrity, prudence and competence of persons having access to the personal data.

Provision of Computer Personnel Services provided by HA, there is a failure to impose a specific obligation on the contractor to comply with the Ordinance[25].

6.17 The level of access privilege to be assigned to different grades of staff is given without any stated principles beyond the two broad principles. Apart from a general grade-and-role-based approach, the process for assigning, changing, reviewing and revoking the access privilege should be strengthened by following prescribed detailed principles and methodology.

Objective of the following recommendations:

To strengthen security measures to reduce the risk of unauthorized or accidental access to patients' data

RECOMMENDATIONS

11. To study the feasibility of using unique identifiers other than HKID numbers for purposes other than authentication of the identities of patients and the prescription of drugs, e.g. in relation to CDARS research purpose; and for matching patients' data kept in other databases of the HA which can be effected through the matching of the hospital number or out-patient's number. The use of other unique identifiers, such as patient numbers or hospital numbers or alternatively, the encryption of the HKID numbers of patients in such manner that are not identifiable outside the HA system whenever these data are to be downloaded onto portable electronic storage devices will reduce the privacy risk associated with human error, such as the inadvertent loss by staff of the equipment containing the data.

12. To consider conducting a security risk assessment to assess the current use of HKID numbers as identifiers, in particular, in relation to their use in appointment slips and gummed labels so as to avoid the accidental disclosure of too much privacy intrusive data.

13. To consider, review and devise a retention policy for electronic data other than clinical data to prevent excessive hoarding of unnecessary data and to consider, review and devise a formal retention policy for the retention of data held outside the main HA system in departments such as the Pharmacy and the Laboratory.

[25] Clause 12 of the Contract

14. To consider and review the policies and practices in relation to the use of portable electronic storage devices by prescribing a mechanism for granting and reviewing the continuing needs by (i) prescribing the period of approval; (ii) requiring specific reasons to be given under the broad category of the "Organizational Need to Know" principle; (iii) prescribing the renewal application procedures; and (iv) keeping logs of records of use for compliance audit purpose.

15. To review the downloading of patients' data created by the staff, e.g. in writing medical reports or letters and documents saved in Microsoft Office and taking them home to continue work. Policies and guidelines should be devised to regulate the taking outside the workplace of patients' data to ensure that (i) extra-sensitive patients' data should not be allowed to be taken outside the workplace; (ii) the patients' data should be de-identified as far as practicable or identifiers (other than HKID numbers) assigned by the HA, such as patients' numbers or hospital numbers are used, which are not identifiable outside the HA system; (iii) the user's own personal computers should be free from spying software and share files software, such as Foxy; (iv) the data should be erased safely after the work has finished; and (v) adequate security protection is provided by the encryption used for handling sensitive personal data, such as when HKID numbers of patients are downloaded.

16. To consider and develop further a prescribed set of procedures with more detailed principles for granting and reviewing access privileges by staff to patients' data to ensure that the access is based only on "Patient under Care" and "Organizational Need to Know" principles.

17. To consider and review the feasibility of prescribing an expiry date of the validity of the passwords used to access CMS or alternatively, to provide for a two-factor authentication, for example, the use of password together with a token for added security.

18. To impose more specific contractual obligation upon third parties who are entrusted with the handling of patients' data, such as the IT contractors and waste disposal contractors to ensure the safe erasure of the data and to prohibit against the further or other use of the data. Personal data should as far as practicable not be allowed to be carried off-site for testing by the IT contractor or staff[26].

[26] Reference is drawn to the recommendations made by the Commissioner in a published report, i.e. Report #R06-2599 on measures to be taken when engaging outsourced contractor and agent. The report can be

IV Privacy Audit

Areas of concern:

6.18 In order to ensure that there is no restriction on the ability to provide prompt clinical care, retrospective reviews will always form an important and essential element of the HA's system. However they must be carried out in a timely (daily, not quarterly) manner and systematically, i.e. with a standardised process and procedure in place to be followed. That is not the current situation.

6.19 There is no regular systematic IT audit being conducted by the HA. There is no process for regular systematic data security monitoring by hospitals or regular security audits conducted by the HA. Although the HA Annual Plan Section 3: Standard 53 requires the implementation of guidelines on the security and confidentiality of medical records and health information, and access to patients' clinical data and that missing records are indexed and reported to Hospital management, this is undertaken in the form of self-assessment by individual hospitals only. The HA does not proactively audit the security standard of each hospital on a timely and systematic basis.

6.20 The yearly audit on compliance of data protection principles reported by the Data Controller does not appear to be based on prescribed methodology. The Hospital management developed a set of Patient Data Privacy Checklists for annual completion by the departments of the Hospital but it does not represent a prescribed procedure required by the HA to be adopted by all hospitals.

6.21 The random audit on open CMS workstations (to ensure that a password is required for entry into the system and auto log-out function is available) is conducted by the Hospital's own IT staff only once a year. On the day of the Inspection, one of the officers of the Commissioner observed in one computer workstation located in the office of the Department of Pharmacy of Ruttonjee Hospital that there were two USB devices left unattended and the workstation was in operation mode (i.e it was not logged out). In response to the query raised by the Commissioner, the Hospital confirmed that it is a stand alone computer not connected to any HA IT system. It does however have Internet and Intranet access for use by the pharmacists only. The Hospital confirmed that no patients' data had ever been stored in this computer and the computer is mainly used to prepare documents such as the Newsletter to staff on drug issues, drug bulletins and reports related to drug usages. The Hospital

explained that there is always a plug-in sensor for the wireless mouse and showed the Commissioner with a photograph to illustrate this setting. The Pharmacy staff confirmed to the Hospital that there has never been any personally owned or hospital supplied USB drive used in the Department. In the absence of other supporting evidence to confirm the improper use of USB drive, the Team could not take further issue on this matter. On the other hand, the Hospital did admit that the workstation in question has no automatic log-out function and it is now considering the feasibility of installing an automatic log-out function on this computer. It demonstrates that more frequent and regular checks should be undertaken.

6.22 The "Red Zone" audit had been discontinued as the HA was concerned that it might contravene DPP 3 by matching the staff-patients' records kept in the CMS with the HR records of the staff. It appears that HA had not given due consideration to the other provisions of the Ordinance, in particular, the option of obtaining consent from the data subjects and the applicability of the exemption provisions under the Ordinance.

6.23 The "Non-Green Zone" audit which is represented by the checking of the audit trail logs to detect any abnormal trend of CMS access behaviour was carried out by individual hospitals according to their own decisions and judgment[27]. No systematic audit and no "auto-alert" criteria have been devised. Nor has there been any regular monitoring. The CDPC, which was formed in 2006 had decided to devise guidelines for systematic audit to be carried out. It has yet to develop a systematic audit methodology to be followed by all hospitals. In addition, as the Green Zone includes data beyond the "Patient under Care"[28] for many hospital staff, there is a need for audit here as well.

6.24 The criteria for the "auto-alert" system should be finalized as soon as practicable so that it can start operating.

---

[27] According tothe Hospital, about 15 audit exercises on the proper use of CMS from 2001 to 2006 were carried out. The work ceased since the formation of the CDPC which decided to take over the audit and to devise general guidelines.

[28] As, according to the definition given by HA, Green Zone access means access to patients' data is supported by face-to-face patient contact or is within a reasonable period of the patient attendance / admission. The period is set by HA as 365 days before / after attendance.

Objective of the following recommendations:

To develop systematic data security audit methodology to be followed by the Clusters and the hospitals

RECOMMENDATIONS

19. To review and devise a regular systematic compliance audit system overseen by the HAHO to be effectively carried out on a timely and regular basis to ensure that there is due compliance with the security policies and practices. Consideration should be given to dedicating a HAHO Corporate System Security Team or to retaining outside independent parties to conduct the audit.

20. Any internal privacy audits to be carried out by individual hospitals should be systematic by adhering to prescribed procedures. A consistent set of checklists / "self-assessment kits" should be developed and applied to all hospitals.

21. To consider and review the present definitions given to Green, Amber and Red Zones to facilitate audits to be conducted as required under the Manual.

22. To consider the need for "Green Zone" audits and to review the mechanism of the "Red Zone" audit and to assess carefully the legal requirements under the Ordinance, in particular, the obtaining of prescribed consent from data subjects and the applicability of the exemption provisions.

23. To expedite the development of a set of "auto-alert" criteria by the CDPC so that any security audit on audit trail logs can be effectively and systematically carried out.

24. To consider making it a mandatory reporting requirement that any audit exercise conducted by any hospital and the result thereof be fully reported to the Cluster and to the HAHO which should oversee the taking of such remedial measures as may be appropriate.

25. Any abnormal access log trails should be linked to a monitoring system that enables retrospective review to be done in a timely (such as daily) and systematic way, i.e. standardized processes which are checked.

V Supervision, Education and Training

Areas of concern:

6.25 Since many of the reported losses of personal data in the HA and elsewhere were caused by human factors, the level of staff privacy awareness has to be improved. This can be achieved by tighter supervision being imposed to monitor the daily operations, such as keeping logs of the use of portable electronic storage devices, supervising the proper and safe erasure of patients' data, monitoring the due observance of data privacy by third parties, such as the IT contractors and paper shredding service company, etc. A good reporting system is also imperative in ensuring that prompt action is taken whenever needed.

6.26 Where erasure of medical records is done by appointed contractors, contractual obligations should be imposed on them to ensure the careful handling of the data to prevent unauthorized or accidental access, processing and use. Corresponding security measures should also be adopted by the HA to ensure that patients' data, contained in hard copies of medical reports or laboratory tests are as far as practicable examined in designated places, and to avoid having these reports being carried around at the risk of inadvertently misplacing them.

6.27 The Team is concerned that no procedures are currently in place to ensure that when removable electronic storage devices are returned after use, all data are erased to industry standard and verified by the Hospital's IT Department.

6.28 The low attendance rate at the seminars and fora organized by the HA gives cause for concern. Whilst this can be partly explained by the shift system in the hospitals, some thoughts should be given as to how the training can be more focused and disseminated to a wider spectrum of recipients. The HAHO should take a more proactive role in organizing and appraising the effectiveness of the seminars and fora on a regular and frequent manner and in devising effective modes that encourage more participation.

<u>Objective of the following recommendations</u>:

To tighten supervision of compliance and give more education and training to staff

RECOMMENDATIONS

26. After the recent loss of patients' data incidents, the HA devised *User Application Form for Secure USB Flash Drive* which applies to the use of USB drives only. Since other portable electronic storage devices may also be provided by the Hospital for use by its staff, e.g. removable hard disk, portable computers, digital cameras, etc., the HA should also consider devising policies and specific application forms governing the use of these other types of portable electronic storage devices.

27. To consider and review the current practice of examining hard copies of medical records and laboratory reports by the medical officers to confine the same to designated places only in order to reduce the incidence of loss through carrying around these documents containing patients' data.

28. In order to ensure that patients' data that are handled in open or insecure areas are sufficiently protected, to consider tightening the security measures and conducting regular supervision for these places.

29. Procedures should be devised to ensure that when removable electronic storage devices are returned after use, all data are erased to industry standard, such erasure to be verified by the Hospital's IT Department.

30. There should be more regular and timely re-issue of the relevant circulars on handling patients' data security to the staff.

31. The existing materials used for the induction courses and on-the-job seminars should be reviewed to ensure that the materials used across the HA network are up-to-date and the attention of staff specifically drawn to the need to safeguard the security of patients' data particularly when data are stored in electronic form.

32. To consider the mode of effective dissemination of seminar materials, e.g. through interactive platforms (e.g. on the Intranet, possibly through self-learning kits) so that more staff can participate.

33. To take steps to ensure that there are "train-the-trainer" programmes in place to ensure the competence of trainers across the HA network in conducting the courses and to assess and appraise their performance.

34. The contractors' (e.g. the IT contractors and shredding service contractors) standard and level of compliance with the data security principle should be made a specific factor for consideration when reviewing or renewing their contracts and where appropriate, to be included as a standard clause in all such contracts.

VI Privacy Impact Assessment

Areas of concern:

6.29 In view of the fact that the HA holds and accumulates a substantial amount of patients' data in electronic form and with the plan for full implementation of the proposed e-Health platform, extra care and precaution is called for in handling patients' data. Careful assessment of the privacy risks is therefore a necessary measure to take before implementing any system for storing and using patients' data. Sufficient privacy safeguards should be explored and implemented to mitigate any adverse impact on personal data privacy that may be caused by implementing the system.

Objective of the following recommendation:

To conduct a privacy impact assessment as a mandatory requirement

RECOMMENDATION

35. Before embarking on any new undertaking or project involving the creation, collection, transfer or storage of patients' data via electronic means for a substantial number of patients or where the nature of the data involved is particularly sensitive, the HA should conduct a privacy impact assessment. Sufficient security safeguards should be implemented to manage the privacy risks posed by the project and the assessment process and steps should be clearly documented.

VII Containment Plan

Areas of concern:

6.30 Upon the occurrence of any data security breach, a data user should take practicable steps to mitigate the loss or likely loss that may be caused to the data subjects. In some of the loss incidents, the Commissioner or the data subject was not informed : they had to learn it from other sources. A public body, like the HA should follow the good governance of transparency and accountability by notifying, where appropriate, the affected individuals and the public of any data security breach incident.

6.31 The Commissioner was pleased to note that as a result of the spate of data loss incidents, new measures were taken by the HA in making known the data loss incidents through its AIRS. This is a good practice to be followed by other health-care service providers.

Objective of the following recommendations:

To give data breach notification upon happening of a data security breach

RECOMMENDATIONS

36. Upon the happening of a data security breach, to take appropriate steps to mitigate the loss that may be caused to the affected individuals by undertaking a quick privacy risk assessment taking into account the nature of the personal data involved, the number of affected individuals and the amount of data lost. When loss is caused by systematic defects or loopholes, to take immediate steps to rectify such defects or loopholes to contain the spread of the loss. Where appropriate, to report the data security breach to the law enforcement agencies for investigation.

37. To notify the individuals affected by the data security breach so that remedial action can be taken by them as they see fit. It is also good practice that the Commissioner's Office be informed so that appropriate regulatory action can be taken.

6.32 The Commissioner takes cognizance of the remarkable speed at which development in high technology is taking place. To impose any strict requirement on the HA to use any specific products on the market or adopt any IT system that has just been developed is an exercise in futility because they will in no time be outdated. Hence, constant and regular reviews to keep pace with technological advances and the privacy problems that they may generate should be the HA's long term security strategy. It is also for the same reason that the recommendations given in this Report are technology neutral and meant to be of general guidance to the HA to promote its compliance with the requirements of the Ordinance[29].

[29] The Ordinance, as enacted, is technology neutral and the data protection principles provided under the Ordinance are of general application.

CHAPTER SEVEN

Conclusion

In making this Inspection Report, I am conscious of the fact that there is an expectation from some quarters that the person or persons responsible for the recent losses of patients' data by various hospitals under the management of the Hospital Authority will be identified. To that extent, they will be disappointed because the primary objective of the Inspection is to enable me to make recommendations.

The investigation of individual losses of data is a separate issue and one in which my office is currently engaged. These investigations are looking in detail at the specific losses, how they occurred and whether they constituted a breach of the Ordinance. They will form the subject matters of separate reports to follow.

After the loss of data incidents, the HA had taken some remedial measures, notably the regulation of the use of USB flash drives by its staff for storing patients' data and putting into place the data breach notification mechanism. These measures, piecemeal in nature, are welcome but insufficient to fully address the deficiencies of its patients' data security system. The repeated losses of data suggested that the HA's patients' data system suffered from grave shortcomings.

It was for these reasons that I found an Inspection of the HA's patients' data system under section 36 of the Ordinance to be necessary. The recommendations given by me after the Inspection should facilitate a comprehensive security review by the HA of its patients' data system. This will, in the long term, help to reduce the incidence of losses that have been all too prevalent during the last few months.

For this Inspection, I chose the Ruttonjee Hospital and the Tang Shiu Kin Hospital (which operate as a combined hospital) as a sample of how the HA manages patients' data security in the hospitals under its control. One of the reasons why it was chosen was that there had been no allegation of data loss against it.

The Inspection has concentrated on examining the HA's policies and practices on the protection of patients' data, the implementation and enforcement of such policies and practice, and the promotion of privacy awareness amongst its staff. My finding is that the HA has been conscientious in devising and designing a patients' data security system that seeks to protect patients' sensitive data. However, the difficulties of administering them in a large organisation like the HA with some 53,000 staff are patently obvious. In the absence of a holistic approach, the profusion of policies, manuals and circulars issued by HA only tends to make it difficult for its

busy medical staff to understand and follow. Proper implementation is hampered as a result. The weakness in enforcement is highlighted by the lack of a principled and systematic privacy audit approach that is applicable across all hospitals. While the attention to auditing privacy compliance at the Hospital was impressive, it has to be recognized that that was largely due to the strenuous efforts and proactive steps taken by some individual members of its senior staff. Whether such good work and goodwill are replicated in other public hospitals remains in doubt. I find, not surprisingly, that the level of privacy awareness among the staff of the HA is inadequate. This is supported by the very many loss of data incidents due to human errors. To remedy this, more training and education are urgently needed.

In this Report, I have made various recommendations in the hope that greater improvement will be made in all hospitals managed by the HA in rendering the data of patients more secure. Mindful that hospitals exist for the primary purpose of saving lives, treating those that are sick and preventing the spread of diseases, I have been very much aware that DPP 4 refers to the requirement for a data user to take "*all practicable steps"* to ensure the protection of personal data in its possession. The recommendations to the HA are practicable and should not unreasonably interfere with the primary purposes of the hospitals but will go far in assuring patients that their personal data will be kept safe. Many of these recommendations are directed to elevating the medical staff's standard of privacy awareness so that any human errors can be substantially reduced. I hope a good balance has been struck between the primary needs of medical care and the requirement that patients' sensitive data are properly protected against unauthorized or accidental access, processing and use.

The question might be asked how an inspection of one out of the many hospitals managed by the HA can provide an accurate representation of the way in which the HA's patients' data system functions. I have looked in detail at only one hospital and the way in which it observes and complies with the principles of data protection under the HA's management. To attain that limited objective, I have deployed more than half of the workforce at my disposal at various times during the Inspection[30]. In an ideal world, I would have liked to carry out more wide-ranging studies of other hospitals within the management of the HA, but resources and financial constraints forced me to consider the most effective way in which to use those resources to meet the urgent problems associated with the losses of patients' data. I came to the conclusion that a detailed inspection of only one hospital of average size and complexity was likely to be a more effective use of those resources than a more cursory consideration of a greater number of hospitals. The public

[30] Details of the team members are found at Annex II.

needed to be reassured of the transparency of the system operated by the HA. I believe that this Report will give them a better understanding of that system.

I sincerely hope that this Report will be of value not only to all public hospitals, but also to private hospitals, and that all can benefit from the example of the Hospital and my recommendations.

In concluding this Report, I wish to acknowledge with thanks the contributions made by the very many people without whose assistance it would not have been possible for me to conduct the Inspection so expeditiously.

The friendly co-operation of the staff of the Hospital has enabled the Inspection to be carried out smoothly. We are very conscious of the amount of extra work relative to the Inspection which they were called upon to perform at short notice over and above their clinical and administrative duties.

I have been fortunate to be supported by a team of loyal staff who have worked very hard to undertake the Inspection. They have displayed a firm commitment to their duties and an enthusiasm to apply their skills to a task which was novel to all.

Last, but most significantly, I owe a special debt of gratitude to the Consultants who so willingly contributed to the work of the Inspection by giving their time and expertise with dedication and good humour. Their invaluable advice is reflected in this Report and will undoubtedly result in an improvement in the way in which patients' data are kept secure within our public hospital system.

RODERICK B. WOO

Privacy Commissioner for Personal Data
Hong Kong SAR

July 2008

Glossary

AIDS	*Acquired Immune Deficiency Syndrome*
AIRS	*Advanced Incident Reporting System - a reporting system serving as a tool to support risk management by facilitating the reporting, classification, analysis and management of incidents.*
Audit Trails	*All electric access to patients' data via HA's IT system is logged. The audit trails may become evidence in legal proceedings and are retained as long as the patient records exists*
Audit Trail Logs	*These are the logged records of the audit trails*
Amber Zone	*This is the security risk level devised by HA. It represents the medium security risk zone where access to patients' data is not covered by the Green or the Red Zones*
CDARS	*Clinical Data Analysis and Reporting System – an electronic system adopted by the HA to retrieve clinical data of patients for the conduct of medical research.*
CDPC	*Cluster Data Privacy Committee*
CEC	*Cluster Ethics Committee*
CMS	*Clinical Management System – an electronic system adopted by the HA to process information, including patients' data, for the provision of medical services*

Commissioner	*The Privacy Commissioner for Personal Data, appointed under section 5(3) of the Ordinance*
Commissioner's Office	*The Office of the Privacy Commissioner for Personal Data established under section 5(1) of the Ordinance*
Consultants	*The list of consultants appointed by the Commissioner to assist in the carrying out of the Inspection. Details are found in Annex II*
Data Controller	*The person(s) nominated by each hospital with the function to ensure compliance with the Ordinance*
Data protection principle	*The data protection principles in Schedule 1 of the Ordinance*
DPP 4	*Data Protection Principle 4 in Schedule 1 of the Ordinance*
Green Zone	*This is the security risk level devised by HA. It represents the low security risk zone where access to patients' data is supported by fact-to-face patient contact or is within a short period of the patient attendance / admission*
HA	*Hospital Authority*
HA Chief Executive	*Chief Executive of the HA*
HAHO	*Hospital Authority Head Office*
HKEC	*Hong Kong East Cluster*
HKID	*Hong Kong Identity Card*

Hospital	*The Ruttonjee Hospital and Tang Shiu Kin Hospital*
HR	*Human resources*
Inspection	*The inspection of the personal data system of HA carried out under section 36 of the Ordinance and mentioned in this Report*
IT Circular	*The Information Technology Circular No. 1/2008 on "Enhanced Measures on Enforcing Personal Data Security" issued by the HAHO on 14 May 2008*
IT Committee	*The IT Development Committee of the Hospital*
Manual	*The Clinical Data Policy Manual of the HA*
Ordinance	*Personal Data (Privacy) Ordinance, Cap. 486, Laws of Hong Kong*
Non-Green Zone	*This is where access to patients' data falls outside the ambit of Green Zone*
Organizational Need to Know Principle	*A principle formulated by the HA for controlling access to patients' data held by it. Under the "Organizational Need to Know" Principle, access to patients' data is allowed for various necessary purposes other than the purpose of Patient under Care*
Patient under Care Principle	*A principle formulated by the HA for controlling access to patient data held by them. Under the "Patient under Care" Principle, health care professionals who are involved in the care of a patient have the right of access to clinical data which is relevant to that care*

Personal Data	*Section 2(1) of the Ordinance defines "personal data" to mean 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*
Personal Data System	*Section 2(1) of the Ordinance defines "personal data system" to mean any system, whether or not automated, which is used whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system.*
Practicable	*Section 2(1) of the Ordinance defines "practicable" to mean "reasonably practicable".*
Red Zone	*This is the security risk level devised by HA. It represents the high security risk zone where access to patients' data carries a high security risk, e.g. access to hospital employees' clinical data or access to data of patients of public interest*
Report	*This Report which is published under section 48(1) of the Ordinance*
Team	*The Inspection Team led by the Commissioner, assisted by the Deputy Privacy Commissioner for Personal Data and other officers from the Compliance Division, the Operations Division and Legal Division of the Commissioner's Office. The Team also includes four Consultants from backgrounds of medical, privacy, information technology and legal fields set out in Annex II with secretariat support.*
USB	*Universal Serial Bus*

Wi-Fi *A trademark for the certification of products that meet certain standards for transmitting data over wireless networks*

Annex I

Hospital Abbreviations

Hong Kong East Cluster	
CCH	- Cheshire Home, Chung Hom Kok
PYNEH	- Pamela Youde Nethersole Eastern Hospital
RHTSK	- Ruttonjee Hospital & Tang Shiu Kin Hospital
SJH	- St. John Hospital
TWEH	- Tung Wah Eastern Hospital
WCH	- Wong Chuk Hang Hospital

Hong Kong West Cluster	
DKCH	- The Duchess of Kent Children's Hospital at Sandy Bay
FYKH	- Tung Wah Group of Hospitals Fung Yiu King Hospital
GH	- Grantham Hospital
MMRC	- MacLehose Medical Rehabilitation Centre
QMH	- Queen Mary Hospital
TWH	- Tung Wah Hospital
TYH	- Tsan Yuk Hospital

Kowloon Central Cluster	
BH	- Hong Kong Buddhist Hospital
HKEH	- Hong Kong Eye Hospital
KH	- Kowloon Hospital
QEH	- Queen Elizabeth Hospital
BTS	- Hong Kong Red Cross Blood Transfusion Service
RC	- Rehabaid Centre

Kowloon East Cluster	
HHH	- Haven of Hope Hospital
TKOH	- Tseung Kwan O Hospital
UCH	- United Christian Hospital

Kowloon West Cluster	
CMC	- Caritas Medical Centre
KCH	- Kwai Chung Hospital
KWH	- Kwong Wah Hospital
OLMH	- Our Lady of Maryknoll Hospital
PMH	- Princess Margaret Hospital
WTSH	- Tung Wah Group of Hospitals Wong Tai Sin Hospital
YCH	- Yan Chai Hospital

New Territories East Cluster	
AHNH	- Alice Ho Miu Ling Nethersole Hospital
BBH	- Bradbury Hospice
NDH	- North District Hospital
PWH	- Prince of Wales Hospital
SCH	- Cheshire Home, Shatin
SH	- Shatin Hospital
TPH	- Tai Po Hospital

New Territories West Cluster	
CPH	- Castle Peak Hospital
POH	- Pok Oi Hospital
SLH	- Siu Lam Hospital
TMH	- Tuen Mun Hospital

Annex II

The Inspection Team

Team Leader

Mr. Roderick B. WOO, Privacy Commissioner for Personal Data

Consultants

1. Professor John BACON-SHONE
   Director, Social Science Research Centre, HKU
   Former Chairman, Law Reform Commission Privacy Subcommittee

2. Mr. Christopher Cheuk CHAN, BBS
   Former Registrar, High Court

3. Dr. HO Chung-ping, MH
   Chairman, Information Technology Committee
   Hong Kong Medical Association

4. Ir. Dr. Samson TAM Wai-ho
   Chairman, Group Sense Ltd.
   Chairman, Information Technology Division, Session 2007/08
   Hong Kong Institute of Engineers

Secretary to the Inspection Team

Mr. Patrick R. MOSS
Former Secretary General, Law Society of Hong Kong

Officers of the Commissioner's Office

(i) The Core team

The Deputy Privacy Commissioner
The Chief Legal Counsel
Acting Chief Privacy Compliance Officer
Chief Personal Data Officer
One Legal Counsel
One Senior Personal Data Officer
Two Personal Data Officers

(ii) The Questionnaire team

One Senior Personal Data Officer
Four Personal Data Officers
Three Assistant Personal Data Officers
One Information Technology Officer
One Administrative Executive

(iii) The Corporate Communications team

The Corporate Communications Manager
The Corporate Communications Officer (Education)
The Corporate Communications Officer (Promotion)

(iv) Administrative support

The Personal Assistant to the Privacy Commissioner
The Executive Assistant to the Deputy Privacy Commissioner
The Personal Secretary to the Legal Division
Three Assistant Personal Data Officers
The Official Language Officer

Annex III

Cluster Data Privacy Committee

Terms of Reference:

1. To formulate and monitor the implementation of policies and guidelines for data privacy and security issues in HKEC in the following areas in accordance with the HA's Clinical Data Policy, other related policies and relevant Ordinance(s):

   i. Managing access controls
   ii. Approving requests for data access
   iii. Conducting access audits
   iv. Investigating possible breaches

2. To advise the cluster management on the continuous quality improvement strategy and action for HKEC-wide data privacy and security

3. To educate and promulgate clinical data privacy to all staff in HKEC

4. To report to Senior Management Committee on other relevant management committees

Annex IV

Cluster Ethics Committee

Terms of Reference

Clinical Ethics

1. To provide leadership and governance on ethical aspects of policy decisions and clinical practice in the Cluster.

2. To drive the development of ethical guidelines on pertinent clinical issues in the Cluster.

3. To generate appropriate principles in guiding the Cluster's policy development, service planning and resource related decisions.

4. To provide advice and support for ethics sub-committees on clinical ethical issues.

5. To raise awareness and enhance professional competence in ethical aspects of clinical decision making through education.

Research Ethics

6. To harmonize clinical research ethics in the Cluster hospitals thorough standard setting.

7. To coordinate training for members of ethics sub-committees.

8. To keep a central registry of clinical trials involving patients of Cluster hospitals.

9. To conduct audit on clinical research ethics related performance in the Cluster.

10. To monitor global developments in clinical research ethics.

Annex V

Corporate Clinical Systems

Patient Care Process	Office in hospitals / clinics	Computer systems being used
Patient Registration	Patient attending Accident and Emergency Department ("A&E"), Admission office & Outpatient counters	IPAS OPAS
Patient treatment	Patient treated at hospitals / clinics (Nursing wards, Outpatient rooms, A&E,..)	AEIS, CMS OTMS, ePR
X-ray Examination & Pathology test	Text examination done at X-ray Department & Pathology Department	LIS, RIS
Pharmacy Dispensing	Drug dispensing at Pharmacy	PMS, PHS

- IPAS – InPatient Administration System
- OPAS – OutPatient Appointment System
- AEIS – Accident & Emergency Information System
- CMS – Clinical Management System
- OTMS – Operating Theatre Management System
- LIS – Laboratory Information System
- RIS – Radiology Information System
- PMS – Pharmacy Management System
- PHS – Pharmacy Supplies System
- ePR – Electronic Patient Record

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

Questionnaire

This Questionnaire is conducted as part of the inspection exercise carried out by the Privacy Commissioner for Personal Data under section 36 of the Personal Data (Privacy) Ordinance on the personal data system of the Hospital Authority ("**HA**") in relation to security of patients' data in Ruttonjee Hospital and Tang Shiu Kin Hospital.

For the purposes of this Questionnaire, (a) "**patients' data**" means personal data that are collected in the process of clinical care, including demographic, administrative and clinical data, whether or not they are stored electronically (e.g. stored in the Clinical Management System (**CMS**)) or in hard copy; (b)"**clinical data**" means personal data that are related to the physical or mental health of an individual and/or the health care that the individual receives; and (c) "**access**" means and includes the coming into contact with (including the collection and creation of) patients' data whether in hard copies or electronic forms.

You are not asked to disclose your identity in completing this questionnaire nor will any identifiable data in the completed questionnaire be passed to your hospital and the HA. Please read the following questions carefully before giving your answers by ticking the box. For some questions, **you may choose to tick more than one box**. Your assistance is appreciated.

Section A – General

1. Your present job type is:

A. ☐ Administrative/Accounting staff
B. ☐ Medical officer
C. ☐ Nursing staff
D. ☐ IT staff
E. ☐ Laboratory staff
F. ☐ Research staff
G. ☐ Allied health care professional (e.g. pharmacist, physiotherapist, speech therapist and occupational therapist)
H. ☐ Others, please specify: _____

2. How long have you been employed by the HA?

A. ☐ Less than 1 year
B. ☐ 1 year to less than 3 years
C. ☐ 3 years to less than 5 years
D. ☐ 5 years or above
E. ☐ Not applicable

3. **How long have you been working in this hospital?**
   A. ☐ Less than 1 year
   B. ☐ 1 year to less than 3 years
   C. ☐ 3 years to less than 5 years
   D. ☐ 5 years or above

4. **In discharge of your job duties, do you have to access patients' data?**
   A. ☐ Yes
   B. ☐ No (Please skip Section B and go to Section C Question 31 directly.)

   <u>If yes</u>, do you have to access clinical data?
   i. ☐ Yes
   ii. ☐ No

<u>Section B – Patients' Data Handling</u>

5. **In what form are these patients' data being handled?**
   A. ☐ Hard copy
   B. ☐ Electronic form (e.g. CMS)
   C. ☐ Others, please specify: _____

6. **Apart from your normal job duties, have you ever received instruction to seek prior approval before accessing patients' data (e.g. for research reason)?**
   A. ☐ Yes
   B. ☐ No
   C. ☐ I don't know

7. **Have you ever been told that there is a distinction between "confidential" and "unclassified" data?**
   A. ☐ Yes
   B. ☐ No

   <u>If yes</u>, by whom?
   i. ☐ During formal training
   ii. ☐ Being informed by my supervisor, whether verbally or in writing
   iii. ☐ Finding it out myself (e.g. on intranet)

8. **Have you ever been told that patients' data can only be accessed under two restricted purposes, i.e. "patients-under-care" purpose and "organizational need-to- know" purpose?**
   A. ☐ Yes
   B. ☐ No

   <u>If yes</u>, by whom?
   i. ☐ During formal training
   ii. ☐ Being informed by my supervisor, whether verbally or in writing
   iii. ☐ Finding it out myself (e.g. on intranet)

9. **If you work in an open area, are patients' data in hard copy in your work area kept secure when not in use?**
   A. ☐ Yes
   B. ☐ No
   C. ☐ Not applicable

10. Is access to patients' data by computer password controlled?

A. ☐ Yes
B. ☐ No
C. ☐ Not applicable

<u>If yes</u>, do you log out when leaving the computer?

i. ☐ Yes
ii. ☐ No
iii. ☐ I rely on auto log-out mechanism

11. Do you ever share your password with other users?

A. ☐ Yes
B. ☐ No

<u>If yes</u>, are you allowed by the hospital to share your password with other users?

i. ☐ Yes
ii. ☐ No
iii. ☐ I don't know

12. Have you ever imported patients' data in the course of your employment within the past 12 months?

A. ☐ Yes
B. ☐ No

<u>If yes</u>, how did you obtain it?

i. ☐ With hard copy
ii. ☐ Via intranet
iii. ☐ Via internet (e.g. email)
iv. ☐ Via electronic devices
v. ☐ Others, please specify: _____

and

Where did it come from?

a. ☐ Colleagues from your hospital
b. ☐ Other hospitals / clinics / organizations under HA
c. ☐ Others, please specify sources: _____

13. Have you ever imported patients' data via email attachment within the past 12 months?

A. ☐ Yes
B. ☐ No

<u>If yes</u>, were these imported data-

i. ☐ Password-protected spreadsheet?
ii. ☐ Encrypted file?
iii. ☐ Others? Please specify: _____

14. Have you ever downloaded or exported patients' data in the course of your employment within the past 12 months?

A. ☐ Yes
B. ☐ No

<u>If yes</u>, was there any password or encryption used?

i. ☐ Yes
ii. ☐ No

<u>If yes</u>, how often was it used?

a. ☐ Always
b. ☐ Seldom
c. ☐ Only when I was told to

15. **If the answer to the above question is "yes", was the downloading or exporting authorized?**
    A. ☐ Yes
    B. ☐ No
    <u>If yes</u>, by whom was the authority given?
    i. ☐ Immediate supervisor
    ii. ☐ The Privacy Committee
    iii. ☐ The Ethics Committee
    iv. ☐ Others, please specify: _____

16. **Have you ever exported patients' data via email attachment within the past 12 months?**
    A. ☐ Yes
    B. ☐ No
    <u>If yes</u>, was there any password or encryption used?
    i. ☐ Yes
    ii. ☐ No
    iii. ☐ Others, please specify: _____

17. **For what purposes were these patients' data exported from the system?**
    A. ☐ Continued medical care
    B. ☐ Research purpose
    C. ☐ System upkeep
    D. ☐ Administration reason (including complaint investigation)
    E. ☐ Others, please specify: _____
    F. ☐ Not applicable

18. **When you exported patients' data from the system, did you de-identify the data before the export?**
    A. ☐ Yes
    B. ☐ No
    C. ☐ Only if I was told to
    D. ☐ Not applicable

19. **Through what means were these patients' data exported?**
    A. ☐ Intranet
    B. ☐ Printing of hard copy
    C. ☐ Email
    D. ☐ Electronic device
    E. ☐ Others, please specify: _____
    F. ☐ Not applicable

20. **If electronic device was used within the past 12 months for importing or exporting of electronic data, did you engage the use of the following portable electronic devices?**
    A. ☐ Floppy disc
    B. ☐ CD/DVD
    C. ☐ USB storage device
    D. ☐ Laptop computer
    E. ☐ Other portable devices, please specify: _____
    F. ☐ Not applicable

21. Was there any encryption function in the portable electronic devices?

A. ☐ Yes
B. ☐ No
C. ☐ Not applicable

<u>If yes</u>, did you use the encryption function when using these portable electronic devices within the past 12 months?

i. ☐ Always
ii. ☐ Seldom
iii. ☐ Never

22. Were these portable electronic devices provided by the hospital for downloading patients' data?

A. ☐ Yes
B. ☐ No
C. ☐ Not applicable

Did you submit the application for downloading?

i. ☐ Yes
ii. ☐ No

<u>If yes</u>, did you indicate the purpose of use of data in the application?

a. ☐ Yes
b. ☐ No
c. ☐ Other comments, please specify: _____
d. ☐ Not applicable

23. Did you return the portable electronic devices after use?

A. ☐ Yes
B. ☐ No
C. ☐ Not applicable

24. Did you erase the patients' data before returning the portable electronic devices?

A. ☐ Always
B. ☐ Never
C. ☐ Seldom
D. ☐ Not applicable

<u>If yes</u>, how did you erase the data?

i. ☐ By whatever software or built-in erasure function of your choice
ii. ☐ By following other erasure procedure recommended by your hospital
iii. ☐ Others, please specify: _____

25. If you had hard copies of patients' data in your possession, what steps did you take to ensure the secure disposal after the purpose of use of those patients' data had been fulfilled?

A. ☐ Shredding them
B. ☐ Passing them to third parties for disposal
C. ☐ Using them as re-cycled papers
D. ☐ Others, please specify: _____

26. Do you ever transfer patients' data exported from the system to places other than your workplace, e.g. your home, other organizations within the HA or other third parties (e.g. persons other than employees of the HA)?

A. ☐ Yes
B. ☐ No

27. Are you allowed to take the patients' data outside your workplace?

A. ☐ Yes
B. ☐ No

If you have ever taken patients' data outside your workplace (whether you are allowed or not), where did you take the data to?

i. ☐ Other hospitals/organizations within the HA
ii. ☐ Your home
iii. ☐ Homes for the aged
iv. ☐ Universities
v. ☐ Others, please specify: _____
vi. ☐ Not applicable

and the reason being:

a. ☐ To perform functions and activities designated by the hospital outside hospital premises
b. ☐ To work at home to meet tight work schedule
c. ☐ To conduct further research at home or at other places
d. ☐ Others, please specify: _____
e. ☐ Not applicable

28. Did you always obtain approval from any person before taking the patients' data outside your work place?

A. ☐ Yes
B. ☐ No

<u>If yes</u>, please specify the title of the approval authority: _____

29. Have you ever stored patients' data on an electronic device owned by you?

A. ☐ Yes
B. ☐ No

<u>If yes</u>, did you submit your electronic device to be managed by hospital IT in the same way as a standard corporate PC?

i. ☐ Yes
ii. ☐ No

<u>If no</u>, did you ensure that your device is free from virus and free from data leakage through social network applications (e.g. Foxy, MSN Messenger, Facebook, FTP and web server)?

a. ☐ Yes
b. ☐ No

30. What patients' identifiers do you usually use when compiling information about the patient in your workstation before transferring the data onto HA's system?

A. ☐ The name
B. ☐ The HKID number
C. ☐ The hospital number assigned to each patient
D. ☐ Others, please specify: _____

Section C – Policies, Guidelines or Practices Governing Patients' Data Handling

31. Are you aware of the existence of any policies, guidelines or practices of the hospital regulating the handling of patients' data?

A. ☐ Yes
B. ☐ No

If yes, are you aware of their contents?

i. ☐ Yes
ii. ☐ No

If yes, how well do you understand their contents?

a. ☐ 1 (I do not understand them.)
b. ☐ 2 (I barely understand them.)
c. ☐ 3 (I fairly understand them.)
d. ☐ 4 (I understand them well.)

32. Are you aware of any policies, guidelines or practices of the hospital regulating the use of electronic devices for importing and exporting patients' data?

A. ☐ Yes
B. ☐ No

If yes, are you aware of their contents?

i. ☐ Yes
ii. ☐ No

If yes, how well do you understand their contents?

a. ☐ 1 (I do not understand them.)
b. ☐ 2 (I barely understand them.)
c. ☐ 3 (I fairly understand them.)
d. ☐ 4 (I understand them well.)

33. Have you ever lost any print-out containing patients' data or the electronic devices containing patients' data?

A. ☐ Yes
B. ☐ No
C. ☐ Not applicable

If yes, have you reported loss of the data or the device to your supervisor or the hospital?

i. ☐ Yes
ii. ☐ No

34. Are you aware of the existence of any policies, guidelines, rules or regulations requiring you to notify the hospital if you lost the patients' data or the devices containing the patients' data?

A. ☐ Yes
B. ☐ No

If yes, are you aware of their contents?

i. ☐ Yes
ii. ☐ No

If yes, how well do you understand their contents?

a. ☐ 1 (I do not understand them.)
b. ☐ 2 (I barely understand them.)
c. ☐ 3 (I fairly understand them.)
d. ☐ 4 (I understand them well.)

35. Prior to May 2008, have you ever received any training on:

A. ☐ Maintaining patients' confidentiality
B. ☐ Personal data privacy protection
C. ☐ Use of electronic storage devices
D. ☐ Electronic Communication Policy

36. Do you find the trainings provided by the hospital adequate to address the security of patients' data?

A. ☐ Adequate
B. ☐ Inadequate
C. ☐ Do not know
D. ☐ Do not care

Section D – The Assessment of the Staff's Level of Awareness of Personal Data Privacy

37. Are staff levels of competence in complying with the privacy policies, guidelines and practices of the hospital an item of assessment included in the annual staff appraisal exercise?

A. ☐ Yes
B. ☐ No
C. ☐ Do not know

38. Are you aware of the existence of a Data Protection Officer in your hospital?

A. ☐ Yes
B. ☐ No

If yes, do you know his roles and responsibilities?

i. ☐ Yes
ii. ☐ No
iii. ☐ Do not care

If yes, what are his roles and responsibilities?

a. ☐ Handling data access requests from patients
b. ☐ Organizing and/or conducting trainings in relation to personal data privacy protection
c. ☐ Distributing policies, circulars and/or guidelines, or practices to staff members concerning patients' data handling
d. ☐ Others, please specify: _____

39. How do you rate your colleagues' level of awareness of protection of patients' data privacy? Please rate on a scale of 1 to 10 with 1 being the lowest and 10 being the highest.

40. How do you rate the measures adopted by the hospital to protect the security of patients' data and prevent unauthorized or accidental access, processing and use? Please rate on a scale of 1 to 10 with 1 being the least sufficient and 10 being the most sufficient.

41. How do you rate your colleagues' level of observance of the requirements of the hospital in safeguarding the security of patients' data? Please rate on a scale of 1 to 10 with 1 being the least satisfactory and 10 being the most satisfactory.

☐

42. Are you aware of any of the following problems in your hospital?

A. ☐ Sharing of passwords with others
B. ☐ Computer not logged out after use
C. ☐ Widespread use of portable electronic devices
D. ☐ Portable electronic devices containing patients' data left unattended
E. ☐ Others, please specify: _____

43. If you have a question about patients' data privacy, what can you do to find out the answer?

A. ☐ By asking my colleagues
B. ☐ By asking my supervisor
C. ☐ By asking the Data Protection Officer
D. ☐ By finding it from the intranet
E. ☐ I don't know
F. ☐ Others, please specify: _____

44. How, in your view, can the existing personal data system of the hospital be improved to ensure patients' data are better protected?

_____

_____

_____

_____

_____

--- END ---

THANK YOU

Annex VI

Results analysis of the questionnaire

Section A – General

1. Your present job type is (107 answers + 0 blank)		
Administrative/Accounting staff	14	13%
Medical officer	15	14%
Nursing staff	41	38%
IT staff	0	0%
Laboratory staff	4	4%
Research staff	0	0%
Allied health care professional	15	14%
Others	19	18%

2. How long have you been employed by the HA? (107 answers + 0 blank)		
Less than 1 year	2	2%
1 year to less than 3 years	6	6%
3 years to less than 5 years	6	6%
5 years or above	93	87%
Not applicable	0	-

3. How long have you been working in this hospital? (107 answers + 0 blank)		
Less than 1 year	6	6%
1 year to less than 3 years	8	7%
3 years to less than 5 years	11	10%
5 years or above	82	77%

4. In discharge of your job duties, do you have to access patients' data? (107 answers + 0 blank)		
Yes	102	95%
No	5	5%
a) <u>If yes</u>, do you have to access clinical data? (97 answers + 10 blanks)		
Yes	82	85%
No	15	15%

Section B – Patients' Data Handling

5. In what form are these patients' data being handled? (103 answers + 4 blanks)		
Hard copy	92	50%
Electronic form (e.g. CMS)	90	49%
Others	1	1%

6. Apart from your normal job duties, have you ever received instruction to seek prior approval before accessing patients' data (e.g. for research reason)? (101 answers + 6 blanks)		
Yes	66	65%
No	34	34%
I don't know	1	1%

7. Have you ever been told that there is a distinction between "confidential" and "unclassified" data? (103 answers + 4 blanks)		
Yes	63	61%
No	40	39%
a) If yes, by whom? (63 answers + 44 blanks)		
During formal training	44	38%
Being informed by my supervisor, whether verbally or in writing	53	46%
Finding it out myself (e.g. on intranet)	19	16%

8. Have you ever been told that patients' data can only be accessed under two restricted purposes, i.e. "patients-under-care" purpose and "organizational need-to- know" purpose? (102 answers + 5 blanks)		
Yes	93	91%
No	9	9%
a) If yes, by whom? (92 answers + 15 blanks)		
During formal training	68	40%
Being informed by my supervisor, whether verbally or in writing	75	44%
Finding it out myself (e.g. on intranet)	28	16%

9. If you work in an open area, are patients' data in hard copy in your work area kept secure when not in use? (103 answers + 4 blanks)		
Yes	96	99%
No	1	1%
Not applicable	6	-

10. Is access to patients' data by computer password controlled? (103 answers + 4 blanks)		
Yes	94	100%
No	0	0%
Not applicable	9	-
a) <u>If yes</u>, do you log out when leaving the computer? (94 answers + 13 blanks)		
Yes	92	90%
No	0	0%
I rely on auto log-out mechanism	10	10%

11. Do you ever share your password with other users? (97 answers + 10 blanks)		
Yes	3	3%
No	94	97%
a) <u>If yes</u>, are you allowed by the hospital to share your password with other users? (3 answers + 104 blanks)		
Yes	0	0%
No	3	100%
I don't know	0	0%

12. Have you ever imported patients' data in the course of your employment within the past 12 months? (102 answers + 5 blanks)		
Yes	44	43%
No	58	57%
a) <u>If yes</u>, how did you obtain it? (44 answers + 63 blanks)		
With hard copy	36	57%
Via intranet	18	29%
Via internet (e.g. email)	1	2%
Via electronic devices	3	5%
Others	5	8%
b) And where did it come from? (43 answers + 64 blanks)		
Colleagues from your hospital	30	44%
Other hospitals / clinics / organizations under HA	25	37%
Others	13	19%

13. Have you ever imported patients' data via email attachment within the past 12 months? (101 answers + 6 blanks)		
Yes	9	9%
No	92	91%
a) <u>If yes</u>, were these imported data (7 answers + 100 blanks)		
Password-protected spreadsheet	4	50%
Encrypted file	3	38%
Others	1	13%

14. Have you ever downloaded or exported patients' data in the course of your employment within the past 12 months? (102 answers + 5 blanks)		
Yes	27	26%
No	75	74%
a) <u>If yes</u>, was there any password or encryption used? (24 answers + 83 blanks)		
Yes	20	83%
No	4	17%
b) <u>If yes</u>, how often was it used? (22 answers + 85 blanks)		
Always	18	82%
Seldom	4	18%
Only when I was told to	0	0%

15. If the answer to the above question is "yes", was the downloading or exporting authorized? (32 answers + 75 blanks)		
Yes	26	81%
No	6	19%
a) <u>If yes</u>, by whom was the authority given? (26 answers + 81 blanks)		
Immediate supervisor	20	59%
The Privacy Committee	4	12%
The Ethics Committee	3	9%
Others	7	21%

16. Have you ever exported patients' data via email attachment within the past 12 months? (101 answers + 6 blanks)		
Yes	10	10%
No	91	90%
a) <u>If yes</u>, was there any password or encryption used? (10 answers + 97 blanks)		
Yes	8	80%
No	2	20%
Others	0	0%

17. For what purposes were these patients' data exported from the system? (98 answers + 9 blanks)		
Continued medical care	21	49%
Research purpose	5	12%
System upkeep	3	7%
Administration reason (including complaint investigation)	13	30%
Others	1	2%
Not applicable	68	-

18. When you exported patients' data from the system, did you de-identify the data before the export? (96 answers + 11 blanks)		
Yes	11	41%
No	11	41%
Only if I was told to	5	19%
Not applicable	69	-

19. Through what means were these patients' data exported? (98 answers + 9 blanks)		
Intranet	13	29%
Printing of hard copy	23	51%
Email	4	9%
Electronic device	2	4%
Others	3	7%
Not applicable	65	-

Portable Electronic Devices

20. If electronic device was used within the past 12 months for importing or exporting of electronic data, did you engage the use of the following portable electronic devices? (99 answers + 8 blanks)		
Floppy disk	3	19%
CD/DVD	3	19%
USB storage device	6	38%
Laptop computer	2	13%
Other portable devices	2	13%
Not applicable	89	-

21. Was there any encryption function in the portable electronic devices? (99 answers + 8 blanks)		
Yes	7	64%
No	4	36%
Not applicable	88	-
a) <u>If yes</u>, did you use the encryption function when using these portable electronic devices within the past 12 months? (7 answers + 100 blanks)		
Always	7	100%
Seldom	0	0%
Never	0	0%

22. Were these portable electronic devices provided by the hospital for downloading patients' data? (99 answers + 8 blanks)		
Yes	7	50%
No	7	50%
Not applicable	86	-
a) Did you submit the application for downloading? (10 answers + 97 blanks)		
Yes	3	30%
No	7	70%
b) <u>If yes</u>, did you indicate the purpose of use of data in the application? (4 answers + 103 blanks)		
Yes	3	100%
No	0	0%
Others	0	0%
Not applicable	1	-

23. Did you return the portable electronic devices after use? (99 answers + 8 blanks)		
Yes	5	63%
No	3	38%
Not applicable	91	-

24. Did you erase the patients' data before returning the portable electronic devices? (99 answers + 8 blanks)		
Always	6	100%
Never	0	0%
Seldom	0	0%
Not applicable	93	-
a) <u>If yes</u>, how did you erase the data? (5 answers + 102 blanks)		
By whatever software or built-in erasure function of your choice	3	43%
By following other erasure procedure recommended by your hospital	1	14%
Others	3	43%

25. If you had hard copies of patients' data in your possession, what steps did you take to ensure the secure disposal after the purpose of use of those patients' data had been fulfilled? (99 answers + 8 blanks)		
Shredding them	45	35%
Passing them to third parties for disposal	68	53%
Using them as re-cycled papers	1	1%
Others	14	11%

26. Do you ever transfer patients' data exported from the system to places other than your workplace, e.g. your home, other organizations within the HA or other third parties (e.g. persons other than employees of the HA)? (99 answers + 8 blanks)		
Yes	9	9%
No	90	91%

27. Are you allowed to take the patients' data outside your workplace? (101 answers + 6 blanks)		
Yes	10	10%
No	91	90%
a) If you have ever taken patients' data outside your workplace (whether you are allowed or not), where did you take the data to? (69 answers + 38 blanks)		
Other hospitals/organizations within the HA	4	44%
Your home	1	11%
Homes for the aged	2	22%
Universities	0	0%
Others	2	22%
Not applicable	61	-
b) and the reason being: (59 answers + 48 blanks)		
To perform functions and activities designated by the hospital outside hospital premises	4	44%
To work at home to meet tight work schedule	1	11%
To conduct further research at home or at other places	0	0%
Others	4	44%
Not applicable	50	-

28. Did you always obtain approval from any person before taking the patients' data outside your work place? (44 answers + 63 blanks)		
Yes	19	43%
No	25	57%

29. Have you ever stored patients' data on an electronic device owned by you? (100 answers + 7 blanks)		
Yes	5	5%
No	95	95%
a) <u>If yes</u>, did you submit your electronic device to be managed by hospital IT in the same way as a standard corporate PC? (7 answers + 100 blanks)		
Yes	1	14%
No	6	86%
b) <u>If no</u>, did you ensure that your device is free from virus and free from data leakage through social network applications (e.g. Foxy, MSN Messenger, Facebook, FTP and web server)? (7 answers + 100 blanks)		
Yes	7	100%
No	0	0%

30. What patients' identifiers do you usually use when compiling information about the patient in your workstation before transferring the data onto HA's system? (90 answers + 17 blanks)		
The name	46	29%
The HKID number	68	43%
The hospital number assigned to each patient	38	24%
Others	5	3%

Section C – Policies, Guidelines or Practices Governing Patients' Data Handling

31. Are you aware of the existence of any policies, guidelines or practices of the hospital regulating the handling of patients' data? (106 answers + 1 blank)		
Yes	104	98%
No	2	2%
a) If yes, are you aware of their contents? (102 answers + 5 blanks)		
Yes	100	98%
No	2	2%
a) If yes, how well do you understand their contents? (101 answers + 6 blanks)		
1 (I do not understand them.)	0	0%
2 (I barely understand them.)	2	2%
3 (I fairly understand them.)	64	63%
4 (I understand them well.)	35	35%

32. Are you aware of any policies, guidelines or practices of the hospital regulating the use of electronic devices for importing and exporting patients' data? (106 answers + 1 blank)		
Yes	93	88%
No	13	12%
a) If yes, are you aware of their contents? (88 answers + 19 blanks)		
Yes	85	97%
No	3	3%
b) If yes, how well do you understand their contents? (87 answers + 20 blanks)		
1 (I do not understand them.)	2	2%
2 (I barely understand them.)	8	9%
3 (I fairly understand them.)	42	48%
4 (I understand them well.)	35	40%

33. Have you ever lost any print-out containing patients' data or the electronic devices containing patients' data? (106 answers + 1 blank)		
Yes	1	1%
No	101	99%
Not applicable	4	-
a) If yes, have you reported loss of the data or the device to your supervisor or the hospital? (3 answers + 104 blanks)		
Yes	1	33%
No	2	67%

34. Are you aware of the existence of any policies, guidelines, rules or regulations requiring you to notify the hospital if you lost the patients' data or the devices containing the patients' data? (106 answers + 1 blank)		
Yes	98	92%
No	8	8%
a) <u>If yes</u>, are you aware of their contents? (95 answers + 12 blanks)		
Yes	92	97%
No	3	3%
b) <u>If yes</u>, how well do you understand their contents? (94 answers + 13 blanks)		
1 (I do not understand them.)	1	1%
2 (I barely understand them.)	8	9%
3 (I fairly understand them.)	37	39%
4 (I understand them well.)	48	51%

35. Prior to May 2008, have you ever received any training on: (93 answers + 14 blanks)		
Maintaining patients' confidentiality	87	38%
Personal data privacy protection	78	34%
Use of electronic storage devices	30	13%
Electronic Communication Policy	36	16%

36. Do you find the trainings provided by the hospital adequate to address the security of patients' data? (105 answers + 2 blanks)		
Adequate	77	73%
Inadequate	13	12%
Do not know	12	11%
Do not care	3	3%

<u>Section D – The Assessment of the Staff's Level of Awareness of Personal Data Privacy</u>

37. Are staff levels of competence in complying with the privacy policies, guidelines and practices of the hospital an item of assessment included in the annual staff appraisal exercise? (106 answers + 1 blank)		
Yes	36	34%
No	31	29%
Do not know	39	37%

38. Are you aware of the existence of a Data Protection Officer in your hospital? (106 answers + 1 blank)		
Yes	85	80%
No	21	20%
a) <u>If yes</u>, do you know his roles and responsibilities? (84 answers + 23 blanks)		
Yes	68	81%
No	13	15%
Do not care	3	4%
b) <u>If yes</u>, what are his roles and responsibilities? (68 answers + 39 blanks)		
Handling data access requests from patients	41	23%
Organizing and/or conducting trainings in relation to personal data privacy protection	63	36%
Distributing policies, circulars and/or guidelines, or practices to staff members concerning patients' data handling	62	35%
Others	9	5%

39. How do you rate your colleagues' level of awareness of protection of patients' data privacy? Please rate on a scale of 1 to 10 with 1 being the lowest and 10 being the highest. (106 answers + 1 blank)		
1	1	1%
2	0	0%
3	0	0%
4	0	0%
5	3	3%
6	5	5%
7	13	12%
8	40	38%
9	22	21%
10	21	20%

40. How do you rate the measures adopted by the hospital to protect the security of patients' data and prevent unauthorized or accidental access, processing and use? Please rate on a scale of 1 to 10 with 1 being the least sufficient and 10 being the most sufficient. (105 answers + 2 blanks)		
1	1	1%
2	0	0%
3	0	0%
4	0	0%
5	3	3%
6	6	6%
7	16	15%
8	29	28%
9	29	28%
10	21	20%

41. How do you rate your colleagues' level of observance of the requirements of the hospital in safeguarding the security of patients' data? Please rate on a scale of 1 to 10 with 1 being the least satisfactory and 10 being the most satisfactory. (106 answers + 1 blanks)		
1	1	1%
2	0	0%
3	0	0%
4	0	0%
5	2	2%
6	3	3%
7	15	14%
8	32	30%
9	27	26%
10	25	24%

42. Are you aware of any of the following problems in your hospital? (56 answers + 51 blanks)		
Sharing of passwords with others	4	4%
Computer not logged out after use	33	31%
Widespread use of portable electronic devices	9	8%
Portable electronic devices containing patients' data left unattended	3	3%
Others	18	17%

43. If you have a question about patients' data privacy, what can you do to find out the answer? (106 answers + 1 blank)		
By asking my colleagues	21	20%
By asking my supervisor	95	89%
By asking the Data Protection Officer	43	40%
By finding it from the intranet	36	34%
I don't know	1	1%
Others	7	7%

44. How, in your view, can the existing personal data system of the hospital be improved to ensure patients' data are better protected?

a) <u>Policies and Guidelines</u>

Policy, guidelines should be more precise, and in layman terms for easy reference of staff.
Forum reminding them the policies / guidelines / 定期檢討 *(regular review)**
More concrete guidelines; 醫院提供電子裝置予 Staff *(the hospital should provide staff with electronic devices)*

b) Implementation

Must seek approval before downloading / copying of patients' data
醫院要各職切實執行有關的指引 *(the hospital should ensure staff compliance with relevant guidelines)*
即日匯報遺失病人資料個案 *(loss of patients' data should be reported on the day of loss)*
載有病人個人資料文件要妥善保管 *(documents containing patients' data should be kept in safe custody)*
Staff must take heed of the rules and regulations for strict compliance; Reduce workload
Supervisors should strengthen supervision on compliance with HA's instruction substantially
不可隨意將病人資料儲存於 USB 手指 *(patients' data should not be unnecessarily stored in USB flash drives)*

c) Resources

Supply sufficient resources (e.g. bags storing patients' data)
To provide a private area to handle patients' data
More efficient computer system to facilitate our work under the privacy ordinance
Patients' allocation (i.e. spacing) improvement
Provide USB with encryption function; regular training
Increase the space so that staff and patients can be further separated, and that documents could be better placed

d) Security Measures

All workstation are screen saver protected with password
Improvement on security of electronic devices
當使用電腦處理病人個人資料後立即登出 *(logout after using the computer system to process patients' data)*； 當使用完病人個人資料文件後立即銷毀 *(documents containing patients' data will be destroyed immediately after use)*
多用紙張去 Cover 病人資料 *(patients' data are covered by paper sheets)*； 減少在工作上製造不必要載有病人資料的名單 *(reduce unnecessary paper lists containing patients' data)*； 減少隨處放置載有病人資料文件 *(documents containing patients' data should not be left unattended wherever possible)*； 同事應多用有密碼保護的電腦文件 *(colleagues should use password protected computer documents)*
(1)OPAS- Auto logout (2)Firewall (virus detected)

e) Audit

Conduct more audits
Regular audit in relation to data protection
Enhance system in order to find out the one who leak the personal data (e.g. time log)
Improve verification procedures

f) Training

More Training
Training should be conducted at regular basis and be made compulsory.
Continuous education; more detailed formal training during induction stage; centralized training programme for different levels, roles
Training for front-line staff, 加強政策的監管 *(to enhance monitoring of policies)*
提升員工有關保障個人資料的意識，加強培訓及提醒員工 *(increase staff awareness in personal data protection by enhanced training and refreshing programmes)*
More training on Personal Data (Privacy) ordinance
More seminar on Personal Data protection
Refresher Training
Organize more training, refreshment
Provide regular training
Have more training about patients' data privacy
There should be more training on protecting patients' data; using encryption system
More training and workshop
More intense staff education
Formal training / education courses in such area
Provide more training
Regular announcement or reminder
Alert the staff more by memo and circulars
More education, provide / inform updated technology devices / technologies
Training to all staff; Remind staff; Clear instruction of authorization to access to data
Arouse the awareness of the staff on personal data collection
To remind and alert the staff

g) Management Consideration

Strengthen the concept of data management of all staffs in hospital
Patients do not need to handle their own films
Adopt unique, anonymous patient identity for general clinical work
Stop using USB device to store patients data
All PC should be connected within the same cluster

h) Satisfied

現時的系統已很足夠 *(the current system is adequate)*
No need enhancement
I think that patients' data are quite well protected in hospital
The existing personal data system of the hospital is quite well.

Annex VI

Explanatory note to the results analysis of the questionnaire

1. A total of 107 questionnaires were returned. Barring a handful of volunteers, the majority of respondents were interviewed face-to-face by the officers of the Office of the Privacy Commissioner for Personal Data.

2. The interviewers respected the free choice of the respondents. Set out below are some of the observations noted from the results of the questionnaires:-

   - For Question 22, one respondent insisted to tick both "Yes" and "No" boxes.

   - Many respondents who chose to tick "Yes" box but refused to continue with the "Yes" path.

   - Despite ticking the "No" box, many respondents chose to continue with the "Yes" path.

   - Others chose to tick "Yes" or "No" plus "Not applicable" boxes.

3. "Not applicable" statistics were excluded from the percentage calculation.

4. As some respondents had picked more than one choice in a question, the total number of choices made for some questions was higher than that who answered the questions. Attached is a statistical summary of the answers made in such questions.

Annex VI

Statistical Summary of the Answers made in Some Questions in the Questionnaire,

Which the total number of choices made was higher than that who answered the questions

(Please insert the Excel table)