協助改善制度

Help improve data systems

「熱線」當值主任感言
Message from Hotline Duty Officer

站在公署的最前線，我見證著市民及機構對私隱的關注日漸提升，同時亦感受到社會大眾對保護個人資料私隱的意識，與日俱增。

我每星期要聆聽數以百計的查詢電話，然而，當查詢者表示滿意我的解答後，我會感到百般欣慰。

曾經有一位查詢者對我說，他打算設立一個網站作招募會員之用，但他對條例的認識有限，很擔心在收集及處理會員的個人資料時，會觸犯《個人資料（私隱）條例》的規定。於是我便就他的情況，向他解釋了各項保障資料原則的規定，並告訴他如何在公署資料豐富的網站內，找到相關的資訊。經我解答後，他的疑慮大大降低，在掛斷電話前，更連番向我道謝。

這份工作，不但令我對條例的認識有增無減，更令我比以前更有耐性及更懂得用心聆聽。我會繼續努力，以誠懇有禮的態度，提供優質及有效率的服務，滿足查詢人士的需要。

陳培玲
助理個人資料主任

At the forefront of the PCPD, I witness the growing concern of the public and private organizations for privacy, as well as the rising awareness of data protection in the community.

I answer hundreds of enquiry calls every week. I feel satisfied whenever my answers meet callers' needs.

An enquirer had called and informed me that he intended to set up a website to collect and handle members' personal information. He knew very little about the Personal Data (Privacy) Ordinance and was worrying about contravening the Ordinance. In response to his concerns, I explained to him the relevant data protection principles and took him to visit the sophisticated website of the PCPD. My reply immediately relieved the anxious enquirer. Before hanging up the phone, he expressed his thanks to me again and again.

This job not only makes me understand the Ordinance better, but also makes me a good listener and a good communicator. I will continue to do my very best to serve the public with courtesy by providing them with quality and efficient service.

Carol Chan
Assistant Personal Data Officer

查詢服務
Enquiries Service

在個人資料方面保障個人的私隱應是香港每間機構的標準政策。這不單只是因為條例規定，亦因為可以帶來更佳的客戶及僱傭關係、更好的資料質素，以及有效的資料處理。公署致力加強這個訊息，並透過查詢服務，就保障資料的良好行事方式，向公私營機構提供指導及意見。

The protection of the privacy of the individual in relation to personal data should be a standard policy for every organization in Hong Kong. Not just because of the legal requirements of the Ordinance, but because it leads to benefits in terms of better customer and employment relations, improved data quality and efficiency of data processing. The PCPD strives to reinforce this message and provide guidance on good data protection practices to all public & private organizations, large and small.

與食物及衞生局會面

私隱專員於2008年4月9日與食物及衞生局常任秘書長（衞生）李淑儀女士及其同事會面，討論長者醫療券所引起的私隱議題。會議的另一討論項目是電子健康記錄發展計劃。常任秘書長與私隱專員探討適當的安排，解決計劃下的私隱議題。

Meeting with Food & Health Bureau

The Commissioner met with Ms Sandra LEE, Permanent Secretary for Health, and her colleagues on 9 April 2008 to discuss the privacy issues arising from the Health Care Vouchers for the Elderly. Another discussion item in the meeting was the Electronic Health Record Development Programme. The Permanent Secretary had explored with the Commissioner the appropriate arrangements for addressing the privacy issues under the Programme.

與香港西醫工會會面

私隱專員於2008年4月17日與香港西醫工會六名醫生會面，討論如何根據條例規定依從查閱資料要求、檢索資料的行政費用、病人記錄的擁有權、儲存/棄置病人記錄，以及使用電腦處理病人記錄的影響。2008年5月，香港西醫工會在其通訊中刊登了是次會議記錄，以供所有會員參考。

Meeting with Hong Kong Doctors Union

The Commissioner met with six medical doctors from the Hong Kong Doctors Union ("HKDU") on 17 April 2008 to discuss how to comply with data access request under the provisions of the Ordinance, the administrative fees for data retrieval, the ownership of patients' records, the storage/disposal of patients' records, and the implication of computer usage in patients' records. In May 2008, HKDU publicized the notes of this meeting in its bulletin for all members' information.

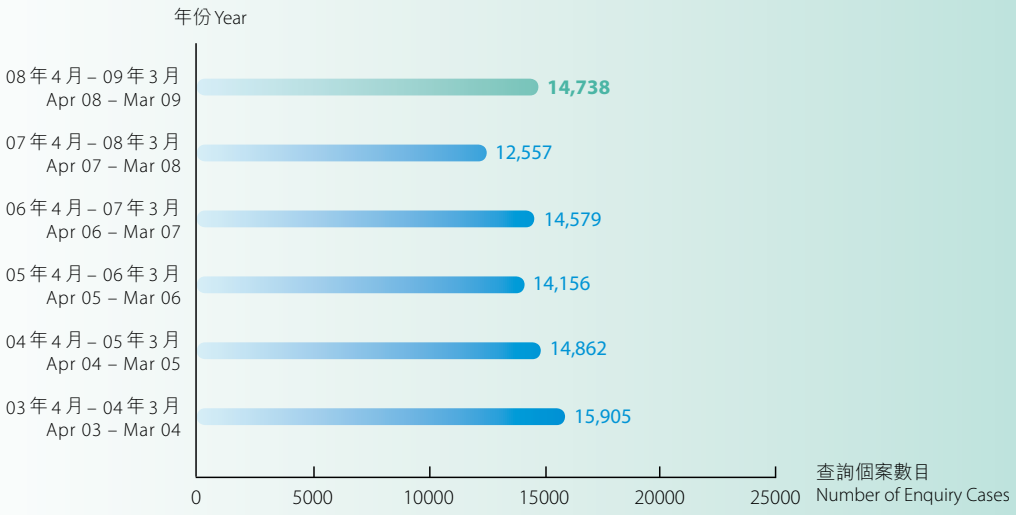
在二零零八至零九年度接獲的查詢
Enquiries Received during 2008-2009

在2008-2009年度，公署共處理14,738宗查詢個案（較去年增加17%），每日平均處理60宗。

A total of 14,738 enquiry cases were handled in 2008-2009 (a 17% increase compared with the previous year). On average, 60 enquiry cases were handled each working day.

圖表 FIGURE 1

每年的查詢個案
Annual Enquiry Caseload



圖表 FIGURE 2

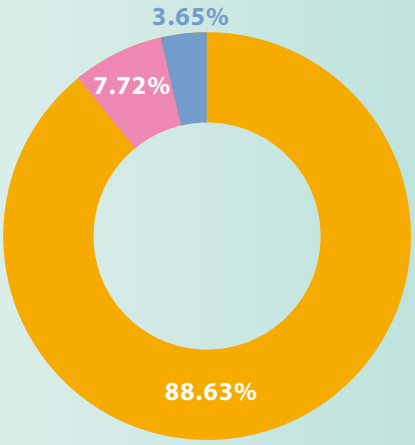
查詢個案的性質
Nature of Enquiry Cases

人力資源管理實務守則 Code of Practice on Human Resource Management	12%
僱主監察僱員活動 Workplace Surveillance	4%
生物辨識科技 Biometrics	1%
個人信貸資料實務守則 Code of Practice on Consumer Credit Data	2%
直接促銷 Direct Marketing	5%
身分證號碼及其他身分代號實務守則 Code of Practice on the Identity Card Number and other Personal Identifiers	4%
查閱資料要求 Data Access Request	9%
追收債款 Debt Collection	2%
與互聯網有關 Internet Related	2%
其他 Others	59%

圖表 FIGURE 3

提出查詢的途徑
Means by Which Enquiries Were Made

熱線 Hotline	88.63%
書面 Written	7.72%
親身查詢 Walk-in	3.65%



大部分的查詢個案(約89%)是透過公署的查詢熱線電話(2827 2827)提出的。

The majority of the enquiry cases (about 89%) were made via the PCPD hotline at 2827 2827.

循規查察行動
Compliance Checks

當發現某一機構的行事方式看來有違條例規定時，私隱專員便會展開循規查察行動。在此等情況下，私隱專員會以書面知會有關機構，指出看來與條例規定不符的事宜，並促請有關機構採取適當的糾正措施。

在大多數情況下，有關機構會主動採取即時措施，糾正涉嫌違例事項。在有些情況中，有關機構會就如何採取改善措施，以免重複涉嫌違例事項，向私隱專員尋求意見。在其他情況下，私隱專員會對涉嫌違例事項進行調查，並採取適當的跟進行動，確保有關機構遵從條例的規定（例如，向有關機構發出執行通知，指令它糾正情況）。

在年報期內，私隱專員共進行了112次循規查察行動，對資料使用者被指違反私隱條例規定的行事方式進行循規查察行動。

大部分循規查察行動（75次）是與私營機構的行事方式有關，其餘37次則關乎政府部門及法定機構。以下是在年內進行的循規查察行動的一些例子。

A compliance check is undertaken when the Commissioner identifies a practice in an organization that appears to be inconsistent with the requirements of the Ordinance. In these circumstances, the Commissioner alerts the organization in writing, pointing out the apparent inconsistency and inviting it, where appropriate, to take remedial actions.

In many cases, the organization takes immediate action to correct the suspected breach. In some instances, advice is sought from the Commissioner on the measures that should be taken to prevent further breaches. Other times, the Commissioner would investigate the matter and take action to ensure compliance with the Ordinance. This might include issuing an enforcement notice to the organization directing it to remedy the situation, for example.

During the reporting year, the Commissioner carried out 112 compliance checks in total in relation to alleged practices of data users that might be inconsistent with the requirements of the Ordinance.

The majority of the compliance checks (75) occurred in the private sector. The remaining 37 related to government departments and statutory bodies. The following examples highlight some of the compliance checks undertaken during the year.

例子 Example

1 一個政府部門的文件透過檔案分享軟件*FOXY*在互聯網上洩漏
Data Leak on the FOXY Network by a Government Department

2008年5月的報章報導，屬於一個政府部門的文件所載有的一些敏感個人資料，透過檔案分享軟件FOXY在互聯網上洩漏。

有關個人資料存於27個文件檔案中，包括內部便函、檔案錄事及其他文件，部分標明「機密」，載有11名訪客／外國人及3名香港居民的姓名、出生日期及身份證明文件類別和號碼，以及一些政府人員的姓名、職級及職銜。

在公署的查詢過程中，該部門與公署人員充分合作，提供有關資訊及資料文件。有關的職員亦就導致資料洩漏的情況向公署作出口供陳述。

該部門承認，是次資料洩漏事件是有關職員疏忽所致。該職員收集了上述電腦文件檔案，作為個案文件的模板，並儲存於家中的私人電腦，以供自學及日後之用，但有關電腦安裝了FOXY軟件。

2008年6月該部門的首長向專員簽署正式承諾書，承諾增加措施，按《個人資料（私隱）條例》的規定加強保障該部門所持有的個人資料的安全。

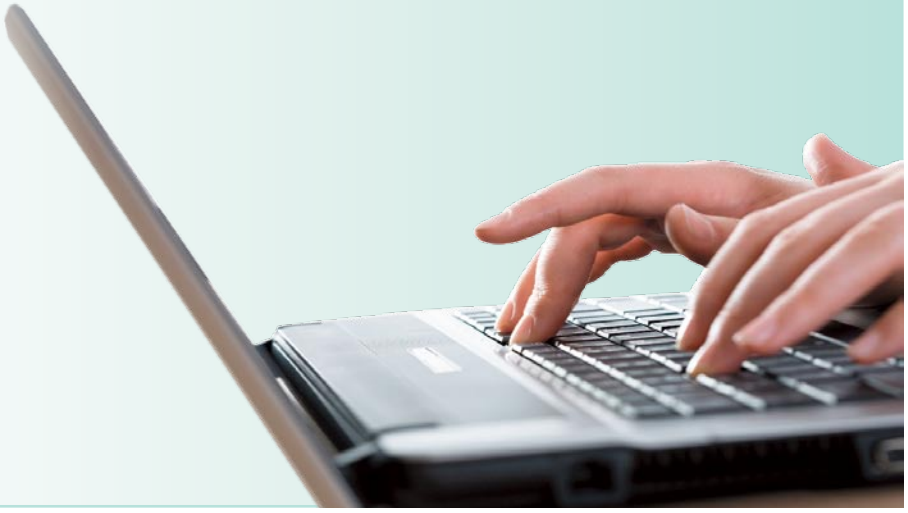
In May 2008, it was reported in the newspapers that some sensitive personal data contained in documents apparently belonging to a government department were leaked on the Internet through a file-sharing software called "FOXY".

The personal data consisted of 27 document files comprising internal memos, file minutes and other documents, some marked "confidential", containing the names, dates of birth, and identification document types and numbers of eleven visitors / foreigners and three Hong Kong residents, as well as the names, ranks and post titles of certain officers.

The department fully co-operated with the Commissioner's officers and provided them with copies of relevant information and materials. The officers involved also gave detailed statements of the circumstances leading to the leakage of the data.

The department acknowledged that the leakage was due to the inadvertence of the relevant staff in collecting and saving the softcopies of the document files as templates of sample case documents for self-study and future use in a personal computer at home, which had installed the "FOXY" program.

In June 2008, the head of the department signed a formal undertaking with the Commissioner to step up measures on data security of the personal data held by the department in compliance with the Ordinance.



例子 Example

2 遺失載有超過50,000名客戶個人資料的電腦伺服器
Loss of a Computer Server Containing the Personal Data of Over 50,000 Customers

2008年5月，一間銀行通知私隱專員，該銀行一間分行遺失一部載有159,000個銀行帳戶（其中超過50,000個屬個人客戶）的電腦伺服器。

該銀行表示，該電腦伺服器被放在分行的地上約半小時沒人看管，而當時有一些工人正進行裝修工程。

為了作出補救，該銀行已向受影響客戶發信致歉，並於2008年7月向私隱專員提交承諾書。

依據承諾書的條款，該銀行會採取所有切實可行的步驟，確保在辦公室裝修期間不會任由載有客戶個人資料的電腦伺服器無人看管，以及受該銀行委托處理客戶個人資料的職員或承辦商是可靠、審慎及有辦事能力的。

In May 2008, a bank brought to the attention of the Commissioner that one of its branch offices had lost a computer server containing about 159,000 bank accounts of which over 50,000 were personal customers.

According to the bank, the computer server was left unattended on the floor in the branch office for about half an hour while there were a number of workers carrying out refurbishment work.

To remedy the situation, the bank had issued apology letters to the affected customers and provided an undertaking to the Commissioner in July 2008.

Pursuant to the terms of the undertaking, the bank would take all practicable steps to ensure that no computer server containing customer personal data be left unattended during office refurbishment and that staff or contractors entrusted by the bank to handle the customers' personal data be reliable, prudent and competent.

例子 Example

3 遺失載有約3,000名病人個人資料的磁碟
Loss of Floppy Disks Containing Personal Data of About 3,000 Patients

2008年7月，本地報章報導一間公立醫院遺失載有約3,000名病人個人資料的11張備份磁碟。儲存於磁碟內的個人資料包括受影響病人的姓名及身份證號碼。

該醫院在回應私隱專員的書面查詢時表示已採取連串補救措施，包括通知所有受影響病人及把所有儲存於磁碟或光碟的個人資料加密。

該醫院亦以書面承諾採取所有切實可行的步驟，保護由它以磁碟或其他類似儲存裝置持有的個人資料不受未獲准許的或意外的查閱、處理或其他使用所影響。

In July 2008, it was reported by local newspapers that 11 back-up floppy disks containing personal data of about 3,000 patients of a public hospital were lost. The personal data stored on the disks included names and identity card numbers of the affected patients.

In response to the Commissioner's written enquiry, the hospital informed that it had taken a number of remedial actions, including notifying all affected patients and encrypting all personal data storing on floppy or optical disks.

The hospital also undertook in writing that it would take all practicable steps to protect personal data held by it in the form of floppy diskettes or other similar storage device from unauthorized or accidental access, processing or other use.

例子 Example

4 遺失載有25,000段電話對話的錄音帶 Loss of an Audiotape Containing 25,000 Recorded Phone Conversations

2008年7月，一間銀行通知私隱專員，該銀行的中國附屬資料處理公司所聘用的外判速遞服務供應商，於廣州至香港的速遞途中遺失一盒載有25,000段電話對話的錄音帶。事件中約有15,000名客戶受影響。

在回應私隱專員的書面查詢時，該銀行提供事件的進一步資料，包括內部對事件的調查報告及速遞服務合約的複本。該銀行亦通知私隱專員它所採取的補救措施。

2008年9月，私隱專員向該銀行發信表達他對事件的初步觀點。該銀行在回覆私隱專員時表示，它會向私隱專員提交承諾書，並把已簽署的承諾書呈交銀行的董事會加簽。

根據承諾書的內容，該銀行會檢討它與外判服務供應商的合約，並盡力在該等合約加入特定條款，規定他們採取措施保障該銀行交予他們的客戶資料。

In July 2008, a bank brought to the attention of the Commissioner that a backup audio tape containing about 25,000 recorded telephone conversations was lost while being couriered from Guangzhou to Hong Kong by an outsourcing courier service provider employed by the bank's affiliated data processing company in China. About 15,000 customers were affected in the incident.

In response to the Commissioner's written inquiry, the bank provided further information on the incident, including an internal investigation report on the incident and a copy of the courier service agreement. The bank also informed the Commissioner of the remedial actions taken by it.

In September 2008, the Commissioner issued a letter to the bank expressing his preliminary view on the matter. The bank replied to the Commissioner that it would provide an undertaking to the Commissioner and that the signed undertaking will be presented to the bank's board of directors for endorsement.

According to the contents of the undertaking, the bank would review the contracts made with its outsourcing service providers and endeavor to incorporate into those contracts specific terms in respect of measures required to be taken by them to protect the customers' data handed to them by the bank.

例子 Example

5 *載有 1,880 名客戶個人資料的電子檔案經電郵被錯發他人*
An Electronic File Containing 1,880 Customers' Personal Data was Wrongfully Sent to an Unintended Recipient by Email

2008年9月，一間保險公司通知私隱專員，該公司錯誤地透過電郵將一個載有約1,880名客戶個人資料的檔案發給一間銀行。

In September 2008, an insurance company informed the Commissioner that a file containing personal data of about 1,880 customers was wrongfully sent to a bank by email.

該保險公司表示，該銀行已刪除該檔案，而引致此事的職員已被書面警告。

According to the insurance company, the wrong recipient had deleted the file and the staff responsible for the incident had been given a written warning.

該保險公司亦通知私隱專員，它已制定行動計劃，以加強資料傳送的保安（密碼保護、檔案管理自動化、加密等）。該公司補充表示，其內部審計師會對公司的資料傳送過程進行特別檢討，焦點是資料私隱。

The insurance company further informed the Commissioner that it had created an action plan to strengthen the data transmission security (password protection, automation of files, encryption, etc.), adding that its internal auditor would conduct a special review of its data transmission process focusing on data privacy.

2008年10月，該保險公司在回應私隱專員的信件時，以書面承諾會遵從保障資料第4原則，加強保安措施，保障其持有的個人資料，避免類似事件再發生。

In October 2008, in response to the Commissioner's letter, the insurance undertook in writing to step up security measures in respect of the security of the personal data held by it in compliance with Data Protection Principle 4 to prevent similar incident from recurring again.

主動調查

如資料違規事件引起公眾極大關注，私隱專員可根據條例第38(b)條主動對事件作出調查，而無需等待投訴人提出投訴。此外，如在循規查察行動時發現有嚴重的違規情況，私隱專員亦會主動調查，以決定應否向有關的資料使用者發出執行通知，指令它改正某行為或採取適當的補救措施。

在截至2009年3月31日的年度，由私隱專員根據第38(b)條主動作出的調查共10宗，其中7宗已經完成。

主動調查醫院管理局(「醫管局」)

2008年5月，私隱專員得悉五間公立醫院共發生九宗遺失載有病人個人資料的電子裝置。遺失的電子裝置包括四個USB記憶體、一個掌上型裝置、一個MP3播放器、一個中央處理器、一部手提電腦及一部相機。涉及10,102名病人的個人資料。

鑑於事件影響香港市民對醫管局保障其個人資料的信心，私隱專員認為為了公眾利益，須調查上述各宗資料外洩事件。

截至2009年3月31日，私隱專員已完成對醫管局的六宗主動調查，這些涉嫌違反資料保安規定的個案全部確立。

Self-initiated Investigation

Where there is a data breach incident of great public concern, the Commissioner may initiate an investigation into the matter under section 38(b) of the Ordinance without waiting for a complainant to come. Also, if serious breach is found during a compliance check, a self-initiated investigation will follow to determine as to whether an enforcement notice should be issued to the data user concerned requiring it to correct certain behavior or adopt appropriate remedial measures.

For the year ended 31 March 2009, the Commissioner had initiated a total of 10 investigations under section 38(b), of which 7 had been completed.

Self-initiated Investigation Against the Hospital Authority ("HA")

In May 2008, it had come to the attention of the Commissioner that there had been nine incidents relating to the loss of electronic devices containing patients' personal data in five public hospitals. The lost electronic devices included four USB memory sticks, one palm handheld device, one MP3 player, one central processing unit, one laptop computer and one camera. The personal data of some 10,102 patients were involved.

Given the impact on the confidence of the people of Hong Kong in the security of their personal data held by HA, the Commissioner considered that it was in the public interest to enquire into each of those data leak incidents.

As at 31 March 2009, the Commissioner completed a total of six self-initiated investigations in relation to HA. They were suspected cases of data security breach. All of them were found substantiated.

對醫院管理局的視察

背景

2008年4月25日，傳媒報導屯門兒童體能智力測驗中心及聯合醫院發生兩宗遺失病人資料事件。涉及病人數目為700人。

2008年5月5日，醫院管理局行政總裁公布，在過去12個月，五間醫院共發生九宗遺失病人資料事件。涉及病人數目增至6,000人。

2008年5月5日傍晚，公署收到威爾斯親王醫院來電，得悉該醫院遺失了一個載有一萬名病人個人資料的記憶體。涉及病人總數增至16,000人。

連串事件反映醫院管理局（下稱「醫管局」）操作的個人資料系統有不足之處，急需視察及檢討，防止日後同類事件重演。

2008年5月8日，專員向醫管局送達通知，準備根據《個人資料（私隱）條例》（下稱「條例」）第36條對醫管局的病人資料系統進行視察。視察的目的是協助專員作出建議，促進醫管局對條例的遵從，視察及建議將會集中在系統方面的保安。

這次是專員首次行使視察權力。對於發生連串遺失病人資料的事件，專員認為為了公眾利益必須這樣做。

律敦治及鄧肇堅醫院（下稱「有關醫院」）被揀選作為實例，以評估醫管局病人資料系統的實施情況。選擇有關醫院的原因包括它並非公署的調查對象。

Inspection on Hospital Authority

Background

On 25 April 2008, two incidents of loss of patients' data in Tuen Mun Child Assessment Centre and the United Christian Hospital were reported. The number of patients involved was 700.

On 5 May 2008, Chief Executive of the Hospital Authority announced that there had been nine incidents of loss of patients' data in the past 12 months in five hospitals. The number of patients involved was increased to 6,000.

In the early evening of 5 May 2008, the PCPD received a call from the Prince of Wales Hospital and learned that a flash drive containing the personal data of 10,000 patients had been lost. This took the total number of patients up to 16,000.

The series of incidents revealed the inadequacies of the personal data system operated by the Hospital Authority ("HA") which needed urgent inspection and review to prevent future similar occurrences.

On 8 May 2008, the Commissioner served notice on HA of his intention to carry out an inspection of HA's patients' data system pursuant to section 36 of the Personal Data (Privacy) Ordinance ("the Ordinance"). The purpose of the inspection was to assist the Commissioner in making recommendations relating to the promotion of HA's compliance. The inspection and the recommendations would focus on the security aspects of the system.

This is the first time that the inspection power is exercised by the Commissioner who finds it in public interest to do so in response to the series of incidents concerning loss of patients' data.

The Ruttonjee and Tang Shiu Kin Hospital ("the Hospital") was chosen as the sample of hospitals to assess the ways that the patients' data system of HA were implemented. The Hospital was not a target of PCPD investigations.

視察小組

專員除了調配公署的職員外，還邀請了四位來自私隱、法律、醫療及資訊科技界別的顧問提供協助。專員帶領小組在2008年5月9日到訪醫管局總辦事處，並於2008年5月16、23及26日和6月12日到訪有關醫院。

視察的進行包括：

- 審閱醫管局有關政策、手冊及指引；
- 會見負責人員及隨機選出約100名員工，請他們填寫特別為是次視察而設計的問卷；及
- 巡視有關醫院的不同部門，巡視實際運作。

Inspection Team

Apart from deploying the regular staff of the PCPD, the Commissioner invited four consultants coming from privacy, legal, medical and information technology fields to assist him in the inspection. The team led by the Commissioner visited the HA Head Office on 9 May 2008 and visited the Hospital on 16, 23 and 26 May and 12 June 2008.

The inspection work included:

- the examination of the relevant policies, manuals and guidelines of HA,
- face-to-face interviews with responsible personnel and some 100 randomly selected staff for completing questionnaire designed for this purpose, and
- the walk through of the various departments of the Hospital to examine the actual operation.

私隱專員對醫管局病人資料系統進行視察。
The Commissioner carried out an inspection of HA's patients' data system.

視察小組觀察所得

從醫管局提供的詳細書面政策及措施看來，它確已制定相當不錯的政策及措施，以保障病人的資料。不過，在沒有整體性的統籌下，大量的政策及措施令工作繁重的醫護人員難以遵從。專員建議對這些政策及措施進行整合、更新及有系統的檢討，協助員工遵從。

為令員工有效遵從保障資料原則及措施的規定，醫管局應對所有醫院採取一套有原則、有系統的私隱審核方法，以便及早發現任何洩漏資料或違反規條例規定的癥兆。

醫管局亦迫切需要提供更多培訓及教育，以提高員工的私隱意識，促使他們遵守條例的規定，以及減低日後再發生人為錯誤導致的違規事故。

建議

專員向醫管局提出了37項建議，目標如下：

- 應有系統地制定、檢討及更新資料保安政策及措施，並有效地傳遞予醫管局員工；
- 清楚界定醫管局聯網委員會的職能，並加強資料管控員的職能，以保障病人資料的安全；
- 醫管局應加強保安措施，以減低未經准許或意外查閱病人資料的風險；
- 醫管局應制定有系統的資料保安審核方法，讓所有醫院遵行；
- 嚴格監督循規情況，為員工提供更多教育及培訓；
- 規定進行私隱影響評估；及
- 在發生違反資料保安事故後，發出資料違規通知。

視察報告

專員於2008年7月22日發表對醫管局個人資料系統進行視察的報告，建議的全文載於該報告的第六章。該報告可以從公署網站(http://www.pcpd.org.hk/chinese/publications/files/HA_inspection_report_c.pdf)下載。

Observations of the Inspection Team

HA has in place fairly good and detailed written policies and practices to deal with patients' data security. However in the absence of a holistic approach, the profusion of these policies and practices have rendered compliance by busy medical staff difficult. The Commissioner suggests that these policies and practices be consolidated, updated and reviewed systematically so as to help its staff to comply with same.

In order to effectively enforce compliance by its staff of the data protection principles and practices, HA should adopt a principled and systematic privacy audit approach across all hospitals so as to detect any early sign of data breach or non-compliance.

There is also a pressing need for HA to raise the level of privacy awareness of its staff by providing more training and education in order to promote compliance of the Ordinance and to minimize the risk of future breaches through human errors.

Recommendations

The Commissioner has made 37 recommendations to HA with the following objectives:

- That there should be systematic formulation, review and updating of the data security policies and practices and their effective dissemination to HA staff;
- That the functional roles to be played by HA's Cluster Committees be clearly defined and that of the Data Controller strengthened to protect patients' data security;
- That the security measures adopted by HA be strengthened to reduce the risk of unauthorized or accidental access to patients' data;
- That HA should develop systematic data security audit methodology to be followed by all hospitals;
- To tighten supervision of compliance and give more education and training to the staff;
- To make it a policy to conduct privacy impact assessment; and
- To give data breach notification upon happening of a data security breach.

Inspection Report

On 22 July 2008, the Commissioner published his report of the inspection of the HA's personal data system. A full version of the recommendations are set out in Chapter Six of the report, which is available for download from the website of PCPD (http://www.pcpd.org.hk/english/publications/files/HA_inspection_report_e.pdf).

核對程序
Matching Procedures

在本年報期內，私隱專員共收到29宗核對程序申請，所有申請均來自公營機構。

During the reporting year, the Commissioner received 29 applications for approval to carry out matching procedures. All the applications were requested by public sector organizations.

經審閱後，其中5宗申請其後撤回。私隱專員根據私隱條例賦予的權力，在有條件的情況下批准了17宗申請。截至2009年3月31日，餘下7宗申請正由私隱專員考慮。

Upon examination, 5 applications were withdrawn subsequently. 17 applications were approved subject to conditions imposed by the Commissioner under the Ordinance. As at 31 March 2009, the remaining 7 applications are under the consideration of the Commissioner.

以下為部份核准的核對程序個案：

The following are some of the matching procedures that were approved by the Commissioner:

提出要求者 **Requesting Parties**	獲准的有關核對程序 **Related Matching Procedures that Were Approved**
房屋協會 Hong Kong Housing Society	公署同意房屋協會進行核對程序，將長者維修自住物業津貼計劃申請人的個人資料，與屋宇署的樓宇安全貸款計劃申請人的個人資料互相比較，以避免有人獲得雙重津貼的情況。 Consent was given to Hong Kong Housing Society to carry out a matching procedure to prevent double benefits by comparing personal data collected by Hong Kong Housing Society from applicants for Building Maintenance Grant Scheme for Elderly Owners with personal data collected by Buildings Department from applicants for Building Safety Loan Scheme.
房屋協會 Hong Kong Housing Society	公署同意房屋協會進行核對程序，將長者維修自住物業津貼計劃申請人的個人資料，與市區重建局的樓宇復修貸款計劃申請人的個人資料互相比較，以避免有人獲得雙重津貼的情況。 Consent was given to Hong Kong Housing Society to carry out a matching procedure to prevent double benefits by comparing the personal data collected by Hong Kong Housing Society from applicants for Building Maintenance Grant Scheme for Elderly Owners with personal data collected by Urban Renewal Authority from applicants for Building Rehabilitation Loan Scheme.
房屋協會 Hong Kong Housing Society	公署同意房屋協會進行核對程序，將長者維修自住物業津貼計劃申請人的個人資料，與房屋委員會的公共屋邨租戶及業主的個人資料互相比較，以確定申請人的申領資格。 Consent was given to Hong Kong Housing Society to carry out a matching procedure to determine the eligibility of applicants for Building Maintenance Grant Scheme for Elderly Owners by comparing the applicants' personal data with the personal data collected by Hong Kong Housing Authority from tenants of public rental housing and owners of subsidized housing.
房屋協會 Hong Kong Housing Society	公署同意房屋協會進行核對程序，將夾心階層住屋計劃申請人的個人資料，與房屋委員會的公共屋邨租戶及業主的個人資料互相比較，以防止有人享用雙重房屋福利。 Consent was given to Hong Kong Housing Society to carry out a matching procedure to prevent double housing benefits by comparing the personal data collected by Hong Kong Housing Society from applicants for Sandwich Class Housing Scheme with the personal data collected by Hong Kong Housing Authority from tenants of public rental housing and owners of subsidized housing.

提出要求者 **Requesting Parties**	獲准的有關核對程序 **Related Matching Procedures that Were Approved**
學生資助辦事處 Student Financial Assistance Agency	公署同意學生資助辦事處進行一次性的核對程序，將2008/09學年內的學生受助人的個人資料，與社會福利署的綜合社會保障援助計劃下的學生受助人個人資料互相比較，以防止一筆過的開學津貼被雙重發放。 Consent was given to Student Financial Assistance Agency to carry out a one-off matching procedure to prevent double subsidy by comparing the personal data collected by Student Financial Assistance Agency from student-recipients of financial subsidies in the 2008/09 school year with the personal data collected by Social Welfare Department from student-recipients of the Comprehensive Social Security Assistance scheme.
強制性公積金計劃管理局 Mandatory Provident Fund Schemes Authority	公署同意強積金計劃管理局進行核對程序，將強積金計劃及職業退休計劃成員的個人資料，與庫務署及教育局轄下同類計劃成員的個人資料互相比較，以確定有關成員符合接受六千元特別供款的資格。 Consent was given to Mandatory Provident Fund Schemes Authority to carry out a matching procedure to determine the eligibility of members of Mandatory Provident Fund schemes and Occupational Retirement schemes to receive a special contribution of $6,000 by comparing the members' personal data with the personal data held by the Treasury and the Education Bureau under similar schemes.
學生資助辦事處 Student Financial Assistance Agency	公署同意學生資助辦事處進行核對程序，將政府大學預科津貼及葛量洪生活津貼的受助人個人資料，與社會福利署的綜合社會保障援助計劃受助人的個人資料互相比較，以避免有人獲得雙重津貼的情況。 Consent was given to Student Financial Assistance Agency to carry out a matching procedure to prevent double benefits by comparing the personal data collected by Student Financial Assistance Agency from applicants for Government Matriculation Maintenance Grants and Grantham Maintenance Grants with the personal data collected by Social Welfare Department from beneficiaries of the Comprehensive Social Security Assistance scheme.
學生資助辦事處 Student Financial Assistance Agency	公署同意學生資助辦事處進行核對程序，將拖欠還款的借款人的個人資料，與人事登記處所持有的個人資料互相比較，以更新該些借款人的地址並進行相關的追討行動。 Consent was given to Student Financial Assistance Agency to carry out a matching procedure to update the addresses of student loan defaulters by comparing the defaulters' personal data with the personal data held by the Registration of Persons Office, thereby facilitating debt recovery.

私隱專員就《醫療改革諮詢文件》向食物及衞生局提交意見
Privacy Commissioner's Submission to Food & Health Bureau in Response to the Healthcare Reform Consultation Document

背景

2008年3月，食物及衞生局（下稱「該局」）展開為期三個月的醫療改革諮詢，徵詢公眾對香港醫療制度未來發展及醫療融資安排的意見。

諮詢文件第4章建議設立電子健康記錄互通系統（下稱「該系統」），讓公私營界別的醫護人員輸入、儲存及檢索病人的醫療記錄。

在世人士的醫療記錄屬於條例第2(1)條下的「個人資料」。任何設立載有病人醫療記錄的電腦系統的建議，必須小心考慮有關系統對條例附表1保障資料第1至6原則所保護的資料私隱權的潛在影響。

2008年6月13日，專員去信該局，從條例規管者的角度對諮詢文件給予意見。

專員的意見

專員請該局留意六項保障資料原則的規定，有關原則包含由收集、保留、使用、保安，以至資料當事人查閱及改正其個人資料的權利的整個資料處理過程。

由於落實該系統會影響個人資料的收集、使用及互通，專員建議進行私隱影響評估，以找出該系統對私隱的實際或潛在影響。私隱影響評估可以協助資料使用者決定如何進行涉及個人資料的科技項目。

專員亦認為在落實該系統後，應定期對該系統進行私隱循規審核，以確保遵從保障資料的規定及防止所收集的資料被濫用。此外，亦應考慮在監管該系統的實務守則中加入審核規定的條文。

結語

專員作為私隱規管者，認為在設計該系統時必須設有足夠的私隱保護措施，例如只收集達致電子健康記錄互通目的所需的最少量資料；透過有效溝通，確保資料當事人完全明白以該系統共用其資料的目的；以及確保萬一資料外洩時對資料當事人所造成的傷害是最少的。

Background

In March 2008, the Food & Health Bureau ("the Bureau") launched a three-month healthcare reform consultation to seek public views on the future development of Hong Kong's healthcare system and financing arrangements.

Chapter 4 of the consultation document proposed to establish an electronic health record sharing system ("the System") with a view to enabling healthcare professionals in both public and private sectors to enter, store and retrieve patients' medical records.

Medical records of living individuals are "personal data" as defined under section 2(1) of the Ordinance. Any proposal to establish a computer system containing patients' medical records warrants careful thought in terms of the potential impact that such system would have upon the data privacy rights enshrined in Data Protection Principle 1 to 6 in Schedule 1 to the Ordinance.

On 13 June 2008, the Commissioner wrote to the Bureau providing it with his comments on the consultation document from his perspective as the regulator of the Ordinance.

The Commissioner's Views

The Commissioner draws the Bureau's attention to the requirements of the six data protection principles, which embody a data processing cycle from collection, retention, use, security to the right of data subjects to access and correct personal data about them.

As the implementation of the System will impact upon the collection, use and sharing of personal data, the Commissioner recommends that a Privacy Impact Assessment ("PIA") be carried out so as to identify any actual or potential effects that the System may have on privacy. PIA helps a data user determine how a technological project involving personal data be proceeded.

The Commissioner also considers it important that Privacy Compliance Audit on the System be conducted regularly after implementation of the System to ensure the compliance of data protection requirements and prevention of abuse of data collected. Besides, consideration should be given to incorporating an audit requirement as a provision in a Code of Practice that governs the System.

Conclusion

As the privacy regulator, the Commissioner takes the view that sufficient privacy safeguards must be in place when designing the System, such as collecting only a minimum amount of data needed to serve the purpose of electronic health record sharing; ensuring data subjects fully understand the purpose of sharing their data through the System by effective communication; and ensuring minimum harm is caused to data subjects in the event of data leakage.