Annex

Hospital Authority (HA)

Following the incidents of loss of patient data, the HA has issued circulars to remind its staff of the importance of protecting the privacy of patients and provided staff with detailed guidelines on the handling and protection of patient data. At the same time, the HA has enhanced its reporting system on loss of patient data and will strengthen the awareness of its staff on the need to protect patients' data through promotional video and training courses.

In addition, HA has started upgrading its patient information system so that any patient data (including name and identity card number) downloaded will be protected through encryption. As an interim measure and before the completion of the system upgrade, no portable electronic storage devices containing patient information may be taken away from the hospitals without prior approval from the Hospital Chief Executives or their delegates.

The HA has also set up a Task Force on Patient Data Security and Privacy to review HA's existing policies and security systems of protection of patient data with a view to recommending improvement measures. The Task Force will complete the review and submit a report to the HA Chief Executive in three months' time.

HA is now in the process of informing the affected patients through interviews, telephone calls or letters.

Department of Health (DH)

Upon the loss of the portable electronic storage devices containing personal data, the DH has instantly emphasized to all staff of the importance of data protection and security, and reminded all service units of the need to comply with data protection regulations.

Except under special circumstances and with the permission of the supervisor of the service unit, no staff may store personal data concerning identifiable individuals in any removable storage medium, or transmit such data out of the Department by any means.

Staff members are required to minimize the storage and transmission of personal data even with permission and must ensure encryption of such data. Data stored in the medium must be deleted immediately after use.

DH will pay close attention to any data protection or security guidelines issued by the Government or the Privacy Commissioner for Personal Data (PCPD), and take necessary actions to strictly comply with such guidelines.

DH took the initiative to report to the PCPD about the data leakage incident. The Department has given written explanations and apologies to the affected children and their families. A hotline is in operation to handle related enquiries.

Civil Service Bureau

On discovery of the loss of a portable electronic storage device which contains the names and post titles of 25 serving civil servants, the Civil Service Bureau has reported the case to the Police and the Office of the PCPD. The storage device contained information on two disciplinary inquiries on alleged misconduct by two civil servants. However no personal data about members of the public were involved. The Bureau has notified and extended apology to all civil servants involved.

After the incident, the Bureau has reviewed its information security measures and issued internal guidelines to remind its staff to comply with the related security regulations at all times. In particular, the guidelines remind staff to keep storage of personal data or classified information to an essential minimum and such data must be encrypted before storage. Such data should not be stored in personally owned devices (including portable electronic storage devices) or personal computers. Where there is an operational need to do so, only portable electronic storage devices with encryption features provided by the government should be used for the storage, handling or transmission of such data. Except with special permission, no staff member is allowed to take classified information away from the office. In case there is a genuine need to do so, the staff will be provided with computers with encryption features, firewall and anti-virus software to handle classified information outside the office through the dedicated Virtual Private Network provided by the government.

Immigration Department (ImmD)

On receipt of report concerning the data leakage incident, the ImmD has instantly taken corresponding measures to reduce its possible impact. Although the data were leaked through a personal computer at the home of the officer concerned, the ImmD took the initiative to immediately inspect all computer terminals of the Department to ensure that the software involved was not installed. At the same time, a home visit was immediately arranged to delete from the officer's computer all the data in question, remove from the computer the software in question and re-format the hard disk. ImmD then made continuous attempts to search the data in question on the Internet for one week and the data in question could no longer be located.

Apart from directing all officers-in-charge of control points to immediately instruct their staff members verbally to observe relevant rules as stipulated in the Personal Data (Privacy) Ordinance and the Government Security Regulations on the day when the incident came into light, the ImmD subsequently re-circulated all relevant internal notices, reminding its staff members to strictly comply with all codes and regulations and to handle personal data and security information with caution. Furthermore, officers responsible for disciplinary matters in all sections have been instructed to request staff members to take all practicable steps to ensure the protection of personal data and to take appropriate disciplinary action against those who breach the rules. These officers were instructed to disseminate the aforesaid message to every staff member of the Department as soon as possible.

The ImmD has considered informing the affected persons. However, 11 of the 14 persons concernd are visitors whose correspondence addresses or telephone numbers are unknown. For the three Hong Kong residents, the leaked documents of two do not contain their personal data and hence their identity cannot be ascertained for further follow-up action. Although the remaining person can be identified, the ImmD is bound by the Registration of Persons (ROP) Ordinance from using the ROP data at will for other communication purposes not prescribed by the law (prescribed purposes under the law include application for registration, renewal and replacement of identity cards, etc.) Should any concerned persons consider themselves being substantively affected by the incident, they may lodge a claim with the ImmD in writing.