For Information
On 30 May 2008

Legislative Council Panel on Information Technology and Broadcasting

Loss of Portable Electronic Storage Devices Containing Electronic Patient Data of the Hospital Authority

Purpose

This paper briefs Members on the recent incidents of loss of portable electronic storage devices containing identifiable patient data from Hospital Authority (HA) hospitals, and provide Members with information on the system in place in HA regarding the security on the handling of electronic patient data and the improvement measures taken.

Background

2. The HA, since its establishment in 1990, has formulated the strategies for the development of IT systems to automate its business processes to support both the front line patient care activities and administration tasks at the back office. Up till now, various IT systems have been implemented in all the 41 hospitals / institutions and over 100 out-patient clinics. Within each hospital, clinical systems are utilized extensively in providing various services including accident and emergency service, in-patient service, out-patient service, laboratory and pharmacy services, etc.

3. The clinical systems capture various data from patients during the provision of the above clinical services and share patient information with other healthcare providers for healthcare related purposes. HA recognizes the importance of maintaining confidentiality of electronic patient data held and has developed various policies, procedure manuals, guidelines and other materials to provide clear guidelines to its staff on the handling of electronic patient data to protect its security.

Summary of Recent Incidents of Loss of Electronic Devices Containing Patient Data

4. Since 1 April 2007 to date, HA has received 10 reports of loss of electronic devices which contain or might contain patient data. These cases concern six hospitals/clinics, ie Pamela Youde Nethersole Eastern Hospital (4 cases), Kowloon Hospital (2 cases), Prince of Wales Hospital (1 case), Sai Ying Pun Jockey Club General Outpatient Clinic (1 case), Tuen Mun Hospital (1 case) and United Christian Hospital (1 case). Of these ten cases, eight were reported to have taken place within hospital/clinic and two outside hospital/clinic premises. The electronic devices lost included five USB

memory sticks, one palm handheld device, one MP3 player, one Central Processing Unit, one laptop computer and one digital camera. Seven of the ten cases are suspected to be theft-related while the remaining three devices were lost. All cases have been reported to the police.

5. It is estimated that a total of 16,000 patients were involved in the ten cases. The data of about 3,000 patients do not contain any personal particulars while the data of around 2,000 patients were protected by password. HA has informed the affected patients through interviews, telephone calls or letters. There has not been any reported case of patient data leakage so far.

HA's Existing Policies and Guidelines on Data Protection

6. Over the past years, HA has developed comprehensive policies and guidelines to protect patient information from unauthorized access. The Clinical Data Policy Working Group set up at the HA Head Office is responsible for formulating policies and guidelines on protection of electronic clinical data, while the Cluster Clinical Data Privacy Committees are responsible for overseeing the implementation of the relevant policies and guidelines at cluster/hospital level.

7. These policies and guidelines cover a wide range of areas, such as the collection, use, access, retention, as well as technical and physical protection of data. It has been HA's established policy that access to patient data will only be allowed based on the following principles -

(i) only health care personnel providing clinical care to a patient will be allowed to access the patient's data under the "patients under medical care" principle;

(ii) access of patient data for activities not directly related to medical care will be allowed strictly on a "need to know" basis, such as for preparing medical reports, conducting clinical researches and clinical audits etc;

(iii) HA staff are requested to replace identifiable patient information and personal particulars with "anonymized identities" as far as practicable when they download the relevant data for work or academic research. If the data to be downloaded contain any identifiable patient information and personal particulars, such data should be encrypted; and

(iv) HA staff are allowed to access the patient data outside hospitals/clinics out of operational needs under certain circumstances, for example, when HA's doctors provide service at residential care homes of the elderly or when community nurses provide service at their patients' homes.

Security and Access Control of HA IT Systems

8. On the IT infrastructure, HA has implemented a secured network infrastructure comprising firewalls, intrusion protection and URL-filtering systems for safeguarding personal data from unauthorized access and malicious attacks.

9. Access to clinical systems is granted only to staff with operational needs in discharging their duties. Access control is governed by parameters including the restriction to same hospital staff only, position and rank of staff, specialty and department of the staff and the nature of their responsibilities, e.g. whether they are providing care to the patient, etc. All access of patient data is recorded in the clinical systems, which renders the use of data by health care staff traceable and prevents illegal access to data. Before staff are granted access right to the clinical systems, they are required to note and sign the patient confidentiality undertaking. Each time when staff log on to the system, a message will be displayed to remind users to maintain patient data privacy and confidentiality.

Promulgations of Guidelines and Training of Staff

10. The above HA policies and guidelines have been promulgated to frontline staff through circulars, internal newsletters and booklets, HA intranet and seminars and briefings on information technology for hospital staff well before the incidents in question.

11. HA has also been promoting staff's awareness of the importance of patient data protection through staff training. For new employees, in particular clinical staff, patient information confidentiality and IT security are included in the orientation program. Patient confidentiality and data access controls are also included in the training for intern doctors on the use of clinical system of HA.

Improvement Measures

12. In response to the recent cases of loss of portable electronic storage device, HA has implemented the following immediate measures to enhance protection of patient data -

(i) HA's patient information system has been upgraded and the downloaded patient data with identifiable patient and personal information (including names and identity card numbers) will be protected through encryption;

(ii) mandatory use of advanced USB flash drives with encryption and password 'lockdown' has been introduced for protecting patient data;

(iii) an Operational Circular on "Enhanced measures on enforcing personal data security" has been issued to remind the staff of the importance of protecting the privacy of patient and provide staff with clear guidelines on how to handle and protect patient data;

(iv) a promotional video and refresher education programs have been launched to educate HA staff on patient data protection; and

(v) the HA's internal Advanced Incident Reporting System has been enhanced. With effect from 19 May 2008, any leakage/loss of patient data must be reported by the relevant staff to the hospital through the Advanced Incident Reporting System as soon as possible, so that management guided remedial action could be taken. While the hospital must submit a preliminary report to the HA Head Office within 48 hours after the incident and explain the situation to the affected patients in two weeks' time. Another Operation Circular on "Policy on the Management of Loss of Electronic Devices Concerning Patient Identifiable Personal Data" has been issued in this regard.

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

14. We will continue to strengthen our security measures to protect patient data while also balancing the clinical and operational need to access such data. Apart from the enhancement measures in paragraph 12 above, we will also implement recommendations from the Task Force as well as those from the Privacy Commissioner of Personal Data, as appropriate.

Advice Sought

15. Members are invited to note the content of this paper.

Hospital Authority
May 2008