LC Paper No. CB(1)1679/07-08(05)

Press Releases

繁體版 | 簡体版 | Email this article | news.gov.hk

LCQ19: Loss of patient data stored in electronic devices
****

Following is a question by the Hon Cheung Hok-ming and a written reply by the Secretary for Food and Health, Dr York Chow, in the Legislative Council today (May 21):

Question:

Regarding the recent several incidents of loss of patient information by health care workers of the Department of Health and public hospitals, will the Government inform this Council:

(a) of the total number of reports received since May last year by the authorities on the loss of patient information by the above health care workers, and among such cases, the number of those in which electronic devices were used for storing the information concerned, as well as the circumstances under which the health care workers involved lost such information;

(b) of the details of the guidelines and codes drawn up by the authorities on access to patients' medical records by health care workers of various ranks (including the circumstances under which health care workers may take information of the patients concerned out of the hospitals or offices, and whether health care workers are allowed to store patient information by any means on their own initiative); and

(c) whether the authorities will consider providing training courses on security of electronic data for health care workers, in order to enhance their awareness of security in handling patient information by means of electronic devices?

Reply:

Madam President,

(a) Since May last year, the Hospital Authority (HA) has received nine reports of loss of patient data stored in electronic devices, of which seven took place in hospitals/clinics and two outside hospitals/clinics. Among these nine cases, six were theft-related while the remaining three were due to negligence.

In the same period, the Department of Health (DH) recorded one incident of loss of identifiable patient data by health care workers. It involved the loss of a USB disk which was previously inserted to a computer in the consultation room of DH's Child Assessment Centre.

(b) To protect patient data, HA has put in place guidelines and codes on a number of areas such as the collection, use, access, retention, as well as technical and physical protection of data. These HA guidelines and codes have been promulgated to frontline staff through circulars, booklets, HA intranet and seminars and briefings on information technology for hospital staff.

It has been HA's established policy that only health care

personnel in charge of a patient will be allowed to access patient data on the "patients under medical care" and "need to know" basis. HA requires its staff to replace identifiable patient information and personal particulars with "pseudo-identifiers" 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. HA allows health care staff 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). HA's relevant policies and guidelines require its staff to take appropriate security and safety measures in handling and storing the patients data.

Besides, HA's Clinical Management System (CMS) has been operating smoothly since its introduction in 1995. All patient data has been properly maintained in the system and there has never been a case of leakage/loss of patient data due to systemic problem of CMS. All access of patient data is recorded in CMS, which renders the use of data by health care staff traceable and prevents illegal access to data. HA has also put in place a reporting system on loss of patient data. With effect from May 19, 2008, any leakage/loss of patient data must be reported by the relevant staff to the hospital through HA's internal Advanced Incident Reporting System as soon as possible, 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.

Following the recent incidents of loss of patient data, HA has implemented a series of measures to enhance the protection of patient data. These include the issue of circulars to staff to remind them of the importance of protecting the privacy of patient and the upgrading of patient information system to protect the downloaded patient data (including names and identity card numbers) through encryption. Before the upgrading of the information system completes, HA staff are not allowed to take away removable electronic storage devices from hospitals without prior approval from the Hospital Chief Executives or their delegates. HA has also 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.

DH also places great emphasis on the protection of patient privacy and has internal guidelines for the handling of personal data. The guidelines are modelled on the data protection principles of the Personal Data (Privacy) Ordinance. Staff of DH's Service Units are required to observe the guidelines, which are applicable to access and use of medical records by health care workers. Among others, the guidelines require that personal data collection and use should be necessary and directly related to the purpose of the Services' function.

To avoid similar incidents from happening again, unless under exceptional circumstances and with the prior approval of the heads of Service, storage of identifiable personal data in any removal storage media, as well as transmission of data away from DH by any means will not be allowed in all DH Service

Units. If approved, staff should keep storage of identifiable personal information in removable storage media or transmission of data to a minimum that is essential for operational needs, and such information must be encrypted. The information should be immediately removed after use.

(c) HA has been promoting staff's awareness of the importance of patient data protection through various channels, such as staff seminars, newsletters, video clips and HA intranet. HA will review and continue to strengthen the measures in this regard including educating the staff about the knowledge of data protection.

In addition, the Civil Service Training and Development Institute has been organising courses for staff on protection of electronic data. DH also regularly re-circulates guidelines on the handling of patient data by electronic means with a view to raising staff's alertness to security. In view of recent incidents, the Department will strengthen training in this area.

Ends/Wednesday, May 21, 2008
Issued at HKT 13:25

NNNN

Print this page