[LCQ13: Electronic Health Record Sharing System](#)

Following is a question by the Hon Charles Mok and a written reply by the Secretary for Food and Health, Professor Sophia Chan, in the Legislative Council today (October 21):

Question:

Last month, the Chief Executive proposed that The University of Hong Kong-Shenzhen Hospital (HKUSZH) be commissioned to provide follow-up consultation service for the following persons: Hong Kong residents who take up long-term residence in Guangdong Province and had scheduled, before the outbreak of the epidemic, follow-up appointments by the specialist outpatient clinics or general outpatient clinics of the Hospital Authority (HA). It has been reported that HKUSZH is discussing with HA the arrangements for Mainland healthcare personnel to access the patient information contained in the Electronic Health Record Sharing System (known in abbreviated form as eHRSS) (the access arrangements). Some members of the public are worried that, in the light of the differences in the regulatory regimes on privacy between the Mainland and Hong Kong, the privacy of patients and their sensitive personal data cannot be protected effectively under the access arrangements. In this connection, will the Government inform this Council:

(1) whether it knows the latest progress of the aforesaid discussion and the modus operandi of the access arrangements; whether it will, in relation to the access arrangements, (i) engage independent third parties to conduct privacy and information security risk assessments and audits, (ii) conduct public consultation and submit to this Council the outcome of the consultation, and (iii) introduce new information security measures for eHRSS;

(2) of the reasons why the current design of eHRSS does not provide options for patients to specify on their own that certain categories of their personal data are not to be uploaded to the system; whether the authorities will make available a "safe deposit box" feature under the access arrangements to allow patients to impose restrictions on the access to and disclosure of their data; if not, of the reasons for that; and

(3) as the Government has made an undertaking to this Council that the protection afforded to the personal data contained in eHRSS would not be less than that stipulated in the Personal Data (Privacy) Ordinance (Cap. 486) for personal data, of the measures in place to maintain the undertaking under the access arrangements, so as to ensure that the patient information of Hong Kong residents is protected against loss and unauthorised or accidental access, use, retention, erasure or disclosure to a third party?

Reply:

President,

Under the impact of the COVID-19 epidemic, some patients of the Hospital Authority (HA) with chronic diseases are unable to return to Hong Kong from the Mainland to receive their scheduled medical consultations at HA's out-patient clinics due to travel restrictions. In view of this, the Food and Health Bureau (FHB), with the support of HA, will set up a special support scheme under which the University of Hong Kong-Shenzhen Hospital (HKU-SZH) will be appointed to provide follow-up consultation services for patients who had scheduled appointments with HA's specialist out-patient clinics and general out-patient clinics before the epidemic.

In consultation with HA, my consolidated reply to the various parts of the question raised by the Hon Charles Mok is as follows:

Under the existing mechanism, patients who have joined the Electronic Health Record Sharing System (eHRSS) or their authorised person can make a data access request (DAR) to the Electronic Health Record Office (eHR Office) under FHB for a copy of their medical records in the eHRSS in accordance with the Personal Data (Privacy) Ordinance (Cap. 486).

To enable patients under the special support scheme to receive continuity of care, the eHR Office will, with the patients' consent and authorisation, make arrangements to assist the patients in passing their medical records to HKU-SZH. Specifically, if a patient participating in the special support scheme has also joined the eHRSS, he/she may, under the established mechanism for data access, make a DAR to the eHR Office for a copy of their medical records in the eHRSS, and give authorisation for the records to be passed to HKU-SZH for use during follow-up consultations for the purpose of receiving better continuity of care. The eHR Office will process the DARs concerned in a centralised manner, and arrange to pass copies of the medical records to HKU-SZH as authorised by the patients. The arrangement for patients to join the eHRSS, make a DAR and authorise the passing of a copy of their medical records to HKU-SZH are all initiated by the patients on their own accord and voluntary in nature. The eHRSS will only make a copy of the individual patient's medical records for passing to HKU-SZH based on the patient's authorisation and DAR (including any requests that specify the type(s) of medical records to be covered).

Under the above arrangement, HKU-SZH is not a healthcare provider under the eHRSS. It cannot directly access any patient records in the eHRSS, and its computer system will not have any interface with the eHRSS. To ensure that patients' privacy is well protected, we will adopt a number of security measures, including after the authorisation and DAR submitted by a patient is confirmed, the eHRSS will create a copy of the medical records for each individual patient, which will be encrypted with different passwords and transferred to an authorised person at HKU-SZH through secured electronic channels using the technologies of public key infrastructure. No system interface with the eHRSS is involved in the process. Furthermore, we will require HKU-SZH to properly and safely use all patient information and

medical records received under the special support scheme, and to put in place appropriate security protection measures. Upon the completion of the special support scheme, HKU-SZH is also required to properly handle the medical records with the consent of the patients concerned.

Since there will be no interface between the computer system of HKU-SZH and the eHRSS, the abovementioned arrangement for the transfer of medical records will not give rise to additional privacy and information security risks to the eHRSS. As far as the eHRSS is concerned, system security has always been our priority. The system has all along been equipped with a number of security technology infrastructures, such as anti-virus software, intrusion detection/prevention, firewall, data encryption, user authentication, digital certificate. Furthermore, in accordance with the Government Information Technology Security Policy and Guidelines, a security risk assessment and audit is conducted every two years on the eHRSS to ensure that the system is properly protected against prevailing security threats.