Bills Committee on
Electronic Health Record Sharing System Bill

The Administration's Response to the Issues
Raised by Members at the Meeting on 19 May 2014

This paper sets out the Administration's response to the request for information raised by members at the meeting on 19 May 2014.

(a) Stage Two of the Electronic Health Record (eHR) Programme

2. The full development plan of the eHR Sharing System (eHRSS) is a 10-year programme which straddles from 2009-10 to 2018-19 and comprising two stages. During Stage One (2009-10 to 2013-14) we focus on the development of:

(a) the core infrastructure for eHR sharing;
(b) standardization of terminologies for use in Hong Kong;
(c) Clinical Management System Adaptation and On-ramp softwares for facilitating connection to sharing platform; and
(d) legal, privacy and security framework

3. As regards Stage Two, our target is to expand the sharable scope of eHR to include:

(a) radiological images – an essential component of modern day patients' record and which is made increasingly possible with advances in digital storage and high speed transmission technology; and

(b) other health-related information such as personal life-style habits, occupation, long term care and treatment plan.

We will also assess the technical feasibility and desirability of adding other enhancement features, and promote the use of clinical management system suitable for Chinese Medicine clinics.

4. During Stage Two, we will conduct research and studies, and may have to implement pilot projects for testing various concepts. In particular, we will look into different design options and assess their

technical and security implications to facilitate patients to more conveniently access their data (viz. a "Patient Portal"). Separately, the outcome of the two-month public consultation on the Legal, Privacy and Security Framework for eHR Sharing launched in December 2011 reflected diverse views on whether the system should provide separate storage of sensitive health records with additional access control (viz. a "safe deposit box"). We undertook to the Panel on Health Services of the Legislative Council that a study on additional access control for sensitive data with reference to overseas experience would be conducted in the next stage of the eHR Programme. We aim to commence the two studies in the first year of Stage Two.

(b) "Safe Deposit Box"

What is a "safe deposit box"?

5. "Safe deposit box" is an electronic data feature which allows the separate storage of certain patient data with enhanced access control. In the context of eHR, this would mean allowing patients to prevent some categories of eHR sharable data from being automatically viewable by healthcare providers even with the general consent of the patients.

6. While recognising the sensitivity of some health data which would warrant extra safeguards, there is a need to balance extra protection for this sensitive data with the completeness and integrity of the eHR to ensure the quality of healthcare delivery.

Arguments for and against provision of such feature

7. During the two-month public consultation in December 2011 to February 2012, diverse views were received on the provision of the "safe deposit box" feature in the eHRSS. The arguments for provision of such feature are mainly centred on:

(a) patients' right to choose the data to be shared;
(b) prevention of possible labelling effect; and
(c) protection of patients from discrimination.

8. As for the arguments against provision of such feature, the major ones are:

(a) Quality of healthcare delivery / Patient safety – the withholding of data from the health records of patients would hamper the completeness and integrity of the eHRSS, thereby undermining the fundamental merit of eHR sharing in enhancing quality of healthcare delivery. The hiding of certain data might even lead to diagnosis errors or wrong treatments.

(b) Health risk to healthcare professionals – for some cases, healthcare professionals would not be able to take precautionary measures to protect themselves and others.

(c) Practical difficulties for patients – It is difficult to determine which particular data should be regarded as "sensitive". Apart from the names of disease, other data contained in a medical record (e.g. name of specialists, medications) may also provide inferences to the "sensitive" data per se.

<u>Current design relating to control access to eHR</u>

9. The current design of the eHRSS has provided flexibility for the patients to control access to their health data. In particular, the implementation of the two levels of consent model provides additional safeguards to participants. By joining the eHRSS (giving "joining consent"), it will not automatically authorize participating healthcare providers (HCPs) to view the health data of the relevant healthcare recipient (HCR). The HCR would need to give a separate "sharing consent" to a particular HCP whom he trusts, such that the HCP could view his eHR from the System. If the HCRs have genuine concern, they could choose to grant consent only to those HCPs that they prefer. Only these HCPs may then upload data to or view the concerned patients' eHR. Consultation record with an HCP who has not been given patient consent will not feature in the eHR.

Study on "safe deposit box" in Stage Two eHR Programme

10. We reported to the Panel at its meeting on 11 June 2012 on the divergent views received during the public consultation on "safe deposit box". In view of the complexity on the issue, we undertook to conduct further study on additional access control over sensitive data with reference to overseas experiences. In this regard, we note that the Australian Medical Association has recently criticized the Australian Personally Controlled Electronic Health Record System (PCEHR) that "the ability of patients to remove or restrict access to information in the PCEHR undermined its usefulness, because doctors could not be confident that it provided the comprehensive medical information needed to make an accurate diagnosis or properly assess the safety of proposed avenues of treatment.". In the meantime, the eHRSS system development would proceed with the basic operational features.

11. As set out in the public consultation document on "The Legal, Privacy and Security Framework for Electronic Health Record Sharing", one of the guiding principle of the framework is that the legislative framework for eHR sharing should be sufficiently versatile and technology neutral to cater for future advancement in health information technology. It is not desirable, nor appropriate, to include the architecture and detailed functionalities (e.g. whether to have the "safe deposit box" function) of an IT system in the legislation, which may hinder the sustainable development of the system. The eHRSS Bill, as currently drafted, does not preclude the provision of such feature in future.

12. Regarding the question on whether to amend the definition of "sharable data" in the proposed section 2 to provide for the possibility that a registered HCR might in future have the right to exclude prescribed HCPs from access to certain part of his/her eHR, we consider that the need to amend the definition has not yet been established at this stage. Actually, the current draft Bill has already provided the flexibility to incorporate future new functions that may facilitate a registered HCR to exercise additional control of access (e.g. use of extra password for certain sensitive health data). Should a decision is made to include the "safe deposit box" function after the study, we will accordingly initiate

system modification and/or review the need for legislative amendments, if any.

13. Given the divergent views on the issue on "safe deposit box" and that we have undertaken the Legislative Council to conduct a study in this regard in Stage Two of the eHR programme, including an express reference that HCR might have the right to exclude prescribed HCPs from access to certain part of his/her eHR in the eHRSS Bill at this stage would pre-empt our further study and could be unfair to stakeholders. We will consult the Steering Committee on eHR Sharing (which comprises representatives from patient groups, healthcare related professional bodies, and the Office of the Government Chief Information Officer) on the findings of the study before making decision.

(c) Ownership of eHR in the eHRSS

14. The eHRSS Bill is concerned with the sharing and using of eHR within the eHRSS. By joining the eHRSS voluntarily, the healthcare recipients (HCR) and the healthcare providers (HCP) (with relevant sharing consent from HCRs) agree to the sharing of relevant health data of the HCR in the System. It does not require any participants to surrender their intellectual property (IP) to the eHR Commissioner.

15. In essence, the eHRSS is a neutral sharing platform which facilitates the provision of health data of HCR by different participating healthcare providers. The System will contain a vast number of health data which may come from a diverse source, such as hospitals, clinics, laboratories, and even possibly from patients in the future (e.g. if some form of "Patient Portal" is to be developed in Stage Two of the eHR programme). If copyright subsists in such compilation of health data, there will be uncertainties as to whom the copyright may be vested in. In any event, the Bill does not affect the legal position regarding the issue of ownership of data or information in the System which is governed under the existing law on, for example IP. Any IP rights relating to the data in the System should be governed by the existing comprehensive legal regime concerning IP protection in Hong Kong. It is therefore not necessary, nor appropriate, to include a definition in relation to the ownership of eHR in the Bill.

16. Ownership / IP rights issues aside, a HCR as the data subject of the relevant personal data stored in the eHRSS, has the right to access his personal data under the Personal Data (Privacy) Ordinance. With a view to enhancing patients' awareness, we are prepared to feature an explanation in the relevant documents such as the "Patient Information Notice" to clarify that they would have access right to their personal data in the eHRSS as data subject. Their right as data subject to access personal data contained in documents written by others kept in the System would not be affected.

Food and Health Bureau
22 May 2014