Bills Committee on Electronic Health Record Sharing System Bill

The Administration's Response to the issues arising from the discussion at the meeting on 24 June 2014

This paper sets out the Administration's response to the issues arising from the discussion of the Bills Committee on the Electronic Health Record Sharing System (eHRSS) Bill on 24 June 2014.

(a) Public Private Interface-Electronic Patient Record Pilot Project

2. The Public Private Interface-Electronic Patient Record (PPI-ePR) pilot project was launched in April 2006 to test the feasibility and acceptability of electronic health record (eHR) sharing. It is a one-way sharing pilot that enables participating healthcare providers in the private sector to access a defined scope of patients' data extracted from the Hospital Authority's electronic patient records. It has thus far enrolled over 360,000 patients and 3,200 private healthcare professionals.

3. In order to safeguard system security and patient privacy, the PPI-ePR pilot has incorporated various special features in its system design and operation workflow. The major ones are highlighted in the ensuing paragraphs.

(i) Enrolment to PPI-ePR

4. Enrolments of healthcare professionals and patients are on voluntary basis. Both healthcare professionals and patients can withdraw from the programme anytime.

5. Before enrolment is confirmed, the identities of relevant healthcare professionals and patients have to be properly authenticated. Healthcare professionals have to provide documentation proof of relevant professional qualification to the PPI-ePR Programme Office for vetting before they join PPI-ePR. As for patients, he/she can use his/her smart

Hong Kong Identity Card (HKIC) for enrolment directly. Otherwise, he/she could submit other valid identity document copy to the PPI-ePR Programme Office for checking. For better security and privacy protection, confirmation letter and a Personal Identification Number (PIN) will be sent to patients upon successful enrolment to PPI-ePR.

(ii) Access to PPI-ePR

6. Access to PPI-ePR is tightly controlled. Healthcare professionals will be issued a security token for future access to the PPI-ePR website upon successful enrolment. In order to log on to the PPI-ePR website, a healthcare professional has to provide his/her user ID, password and a security token generated password for authentication (two-factor authentication).

7. To access individual patient's clinical record in PPI-ePR, a healthcare professional has to further provide the HKIC number of the patient, together with a PIN controlled by a patient. To enhance security and privacy protection, the system will generate an SMS to the patient's registered mobile number to notify the patient of every access by the healthcare professional. The patient may make enquiries / complaints to the PPI-ePR Programme Office whenever he/she has doubts about any access to his/her patient records. A patient may request to change his/her PIN whenever he/she wants to do so. All accesses to PPI-ePR are logged and can be audited when necessary.

(iii) System Infrastructure

8. Personal and sensitive data such as name, address, HKIC number, user password and patient PIN stored in the system are encrypted. The PPI-ePR database is securely segregated from the Hospital Authority internal systems and is protected by multi-layer firewalls. Best practice security protection tools such as intrusion prevention system, anti-virus / anti-malware software and network monitoring solution have been installed to protect the system.

9. Security risk assessment and privacy impact assessment have

been conducted for PPI-ePR.

(iv) Experience Acquired for eHRSS

10. The design and development of eHRSS have taken into consideration the experience of PPI-ePR. Most of the privacy and security measures of PPI-ePR have been adopted or strengthened in the design of eHRSS. Participation in eHRSS will also be voluntary in nature. Data to be shared will be confined to a limited scope. Verification of the healthcare professional's registration status will be automated and done every time an access to eHRSS is made. The SMS notification and two-factor authentication arrangements will be similarly provided. Participating healthcare providers must conform to stringent security and connection requirements. The proposed eHRSS-specific legislation will provide additional protection for participating patients.

(b) Privacy Concerns

11. At the meeting on 24 June 2014, the Privacy Commissioner for Personal Data (PCPD) briefed the Bills Committee on his major comments / concerns regarding the eHRSS Bill. Details are set out in his written submission dated 22 May 2014 (CB(2)1580/13-14(03)). The issues raised by PCPD at the meeting and in his written submission include the following –

(i) sharable scope of eHRSS;
(ii) "need-to-know" principle;
(iii) exclusion of data (viz. "safe deposit box" feature);
(iv) registration of healthcare providers;
(v) persons authorized in writing to make Data Access Request; and
(vi) offences

In the Administration's response issued on 11 June 2014 (CB(2)1775/13-14(02)), we have set out relevant background, explanation of the policy intent, and our stance on the comments and suggestions raised by PCPD.

12. At the meeting on 24 June 2014, PCPD raised only two further follow-up queries / suggestions. First, he enquired about the SMS notification arrangement. In this regard, we have mentioned in previous meetings that when a participating healthcare recipient (HCR)'s eHR in the system has been accessed, the eHRSS will issue a SMS notification to inform the relevant HCR that his/her eHR has been accessed by which particular healthcare provider. This alert arrangement will enable the HCR to make enquiries/complaints to the future Commissioner for the Electronic Health Record if he/she has doubts about any access. As all access to a HCR's eHR in the eHRSS by healthcare providers and healthcare professionals will be logged and traceable, the eHR Office could retrieve the log when handling the complaint / enquiry by an HCR.

13. Another elaborative suggestion made by PCPD at the meeting was to ask the Administration to consider following the practice in Australia where "misuses of eHR" can be subject to a punishment of "civil penalty". We have studied the example quoted and noted that in Australia, civil penalty provisions are described as a hybrid between the criminal and the civil law. Contravention of a civil penalty provision is not an offence. Under the Australian's regime, the regulator may apply to the court for an order that an entity has breached a civil penalty provision. If the court is satisfied that the entity has breached that civil penalty provision, the court may order the breaching entity to pay the government the pecuniary penalty specified in the civil penalty provision. Generally speaking, the imposition of a financial penalty similar to "civil penalty" in Australia is not common in our legal regime.

14. Misuse of personal data in Hong Kong is generally governed by Data Protection Principle (DPP) 3 of the Personal Data (Privacy) Ordinance (the Privacy Ordinance). PCPD may issue an enforcement notice to direct the relevant data user to remedy contravention of DPP and failure to comply with an enforcement notice is an offence. We understand that there was a proposal to subject contravention of a DPP to monetary penalty in the review of the Privacy Ordinance in 2011. It was not pursued because the majority view of the comment received on this

proposal in public consultation was against it. The main reasons include:

(i) it is uncommon for non-judicial bodies to have statutory power to impose monetary penalties;
(ii) the DPPs are couched in generic terms and can be subject to a wide range of interpretations. Whether an act constitutes a serious contravention of a DPP is a matter of subjective judgment. There will be difficulties in enforcement if "serious contravention" of DPPs is not objectively and specifically defined;
(iii) it may not be desirable to vest in a single authority with both enforcement and punitive functions. The roles of investigation, prosecution and adjudication should be performed by different institutions for checks and balances; and
(iv) there is no strong evidence showing that the present system is not working effectively to serve its purpose and therefore a drastic expansion of the PCPD's powers is not justified.

The eHR contains personal data of the relevant HCRs and misuse of eHR is covered by the DPPs under the Privacy Ordinance. The above considerations are therefore very relevant to any proposal regarding penalty for general "misuse of eHR".

15. In the Administration's response issued on 11 June 2014 (CB(2)1775/13-14(02)), we have highlighted that the term "misuse" carries a broad meaning. There are different extents and various scenarios of "misuse" and it is debatable whether all "misuses" should be penalized or even criminalized. In the absence of clear public consensus and legal certainty, it may not be appropriate to empower the eHRC, a non-judicial authority, to impose monetary penalty generally on "misuses of eHR data" couched in broad terms.

Food and Health Bureau
July 2014