LEGISLATIVE COUNCIL

Bills Committee

Electronic Health Record Sharing System Bill

Purpose

This paper sets out the major concerns of the Privacy Commissioner for Personal Data ("**PCPD**") regarding the Electronic Health Record Sharing System Bill ("**Bill**") submitted by the Food and Health Bureau to the Legislative Council on 17 April 2014.

General Comments

Enactment of specific legislation

2. There is little doubt that an Electronic Health Record Sharing System ("**System**") for access and sharing of participating patients' health data by authorised healthcare providers will provide collaborative patient-centred care more efficiently. But it also poses serious challenges to privacy and data protection.

3. The Personal Data (Privacy) Ordinance ("**PDPO**") (Cap. 486) provides general protection to personal data privacy in Hong Kong, regardless of the nature of the personal data. Health data being shared under the System is inherently sensitive and special care is therefore warranted. To ensure adequate protection, the PCPD supports the enactment of a specific legislation to regulate the System.

Compatibility with the PDPO

4. It is of paramount importance that the privacy protection offered to the healthcare recipients' personal data collected, maintained and used in the System would not be less than those provided under the PDPO and that the

PCPD can exercise oversight using his enforcement powers under the PDPO. The Bill must therefore be compatible with the PDPO so as not to prejudice the performance of the functions and the enforcement powers of the PCPD in respect of the healthcare recipients' electronic health records ("**eHR**"s) shared under the System.

5. Section 37(1) of the Bill provides that the PCPD shall perform the functions or exercise the powers under the PDPO in relation to the personal data maintained in the System subject to the conditions set out in sections 37(2) and 38. PCPD's comments on these conditions and other concerns are set out in the paragraphs below.

Specific Areas of Concern

Sharable Scope and Exclusion of Data

6. The System envisaged under the Bill will operate in a manner that is conducive to excessive sharing of the eHR data.

7. Firstly, the sharing consent by a healthcare recipient is given to a prescribed healthcare provider, not to specified units or personnel of the healthcare provider. Where the healthcare provider is a hospital or a healthcare chain providing comprehensive healthcare to the healthcare recipient, all medical professionals of the healthcare provider attending the recipient could access all of his eHR data. This begs the question whether some compartmentalisation of data sharing should be introduced based on the "*need-to-know*" principle. For example, it is doubtful whether a dentist providing general dental treatment to a patient needs to know his ophthalmic data.

8. The Administration has stressed that the System will operate in such a manner that data access will only be made on a *"need-to-know"* basis. The PCPD advocates that this cardinal principle should be duly incorporated in the

Bill.

9. It should be noted that compartmentalisation of data sharing should in any event be a design feature of the System. This stems from the requirement under section 12(6) of the Bill that in a situation of healthcare referral where a prescribed healthcare provider refers the healthcare recipient to another prescribed healthcare provider, the first-mentioned provider may only provide to the second-mentioned provider any sharable data of the recipient *relevant to the referral* and the latter may only obtain from the System any sharable data of the recipient *relevant to the referral*.

10. With compartmentalisation of data sharing duly incorporated in the System at the design stage, the provision of a *"safe deposit box"* that allows the separate storage of certain patient data with enhanced access control should not overburden the cost and operation of the System. The PCPD strongly supports this concept as it respects the healthcare recipient's right of self-determination of his health data and protects the recipient from discrimination which otherwise could result from inadequate access control of particularly sensitive health data such as psychiatric diseases/ mental conditions or hereditary diseases.

11. The downside of providing a *"safe deposit box"* is of course, that the lack of full disclosure of health data might affect the quality of the healthcare provided to the recipient. This clearly needs to be explained to the healthcare recipient joining the System so that he is making a decision in a well-informed manner. Otherwise, the recipient should be left alone to make his choice. After all, the recipient's participation in the System is entirely voluntary and the duty of any healthcare provider is always to do its best based on whatever health data that can be made available, regardless of its completeness.

Registration as Healthcare Providers (Part 2 Division 4 of the Bill)

12. Section 17(5) of the Bill sets out the types of applicants that are

eligible for registration as healthcare providers that are entitled to sharing eHR under the System. Section 17(5)(a) to (f) of the Bill requires either the employment of healthcare professionals by the eligible applicants or their registration under relevant healthcare-related legislations. There are further provisions which empower the eHRC to exercise discretion in accepting registration. Under section 17(g), the eHRC may allow the registration of applicants who *"directly or indirectly provides healthcare"*. Under section 20 of the Bill, the eHRC may register a government bureau or department that *"involves providing healthcare"* (to the exclusion of the Department of Health). The PCPD's concern is how the eHRC will exercise his discretion under these loosely defined situations which would in effect widen the sharing of the healthcare recipients' eHRs.

*Data Access Request (**"DAR**") and Data Correction Request ("**DCR**")(Part 4 of the Bill)*

13. Data access and correction rights are crucial for the protection of an individual's personal data privacy. They are protected under DPP6 in Schedule 1 and other more specific provisions in Part V of the PDPO.

14. Section 38 of the Bill specifically excludes the application of section 17A of the PDPO to the eHR maintained in the System. The implication is that "*a person authorised in writing*" by a healthcare recipient would not be allowed to make a DAR or DCR on the recipient's behalf for his eHR maintained in the System.

15. The PCPD objects to this provision. Denial of healthcare recipient's right to appoint someone in writing as *"relevant person"* to pursue a DAR or DCR will affect adversely the recipients' autonomy in handling his personal data. This is particularly problematic where the healthcare recipient falls sick and requires assistance from others in pursuing the requests. Further, despite the proposed section 38 which applies to the healthcare recipients' health data under the System only, the recipients are still entitled under the PDPO to

exercise the rights to data access and correction through their authorised persons in relation to their health data maintained separately with other healthcare providers such as the Hospital Authority ("**HA**"). This inconsistent treatment of health data under the two different systems but belonging to the same healthcare industry is bizarre.

Offences relating to accessing, damaging or modifying data or information (Part 5 of the Bill)

16. Section 41 of the Bill introduces an offence of knowingly causing a computer to perform a function so as to obtain unauthorised access to data or information contained in an eHR. Section 41(1) expressly defines the "*unauthorised access*" to be one that is performed through the function of a computer such as hacking into the System or using stolen log-in particulars. However, it is conceivable that unauthorised access may be obtained through means other than the use of a computer. For example, where a healthcare professional omits to log out of the System after viewing the eHR of a healthcare recipient, unauthorised access of the eHR may be gained by third parties taking advantage of the situation. To provide for comprehensive protection of eHR, the Administration is requested to consider extending the scope of the offence to include unauthorised access by any means.

Creating an offence against misuse of eHR data (Part 5 of the Bill)

17. While unauthorised access to the eHR through the use of computer is an offence under section 41, no offence is proposed under Part 5 of the Bill for misuse of the data for purposes unrelated to the healthcare of the healthcare recipients, except for the specific offence created under section 46 of the Bill to prohibit against the use of the eHR data for direct marketing purpose. This is an omission which needs to be addressed, particularly as the person misusing the eHR data could be different from the person making the unauthorised access in the first instance.

18. Unless the specific conditions under section 64 of the PDPO governing the disclosure of personal data obtained without data user's consent are fulfilled[1], misuse of personal data is generally governed by DPP3 in Schedule 1 of the PDPO. Contravention of DPP3 itself is not an offence. The PCPD may issue an enforcement notice to direct the relevant data user to remedy the contravention. The data user will only commit an offence if he fails to comply with the enforcement notice. Such enforcement measures are not strong enough to protect the very private and sensitive data of eHR. The PCPD therefore invites the Administration to consider creating a specific offence to govern misuse of eHR data.

Limitation of liability (Part 6 Division 3 of the Bill)

19. Under section 57(2) of the Bill, the eHRC is not obliged to inspect, or commit to inspect, an electronic medical record system to ascertain (1) whether the Electronic Health Record Sharing System Ordinance ("**Ordinance**") is complied with; and (2) whether any sharable data provided to the System is accurate. The justification for this limitation of public liability is not explained in the Legislative Council Brief.

20. The PCPD objects to this proposed limitation. First, it belittles and discredits the eHRC's statutory functions to regulate and supervise the sharing and use of eHR (section 48(1)(b)) among the registered healthcare providers and to supervise their compliance with the Ordinance (section 48(1)(c)).

21. Secondly, it could effectively reduce the PCPD's sanctioning power that may be invoked against the eHRC to ensure his compliance with the PDPO. For example, as a data user, the eHRC is obliged under DPP4[2] in Schedule 1

[1] Under section 64 of the PDPO, it is an offence for a person to disclose any personal data of a data subject obtained from a data user without the latter's consent and with an intent to (i) obtain gain for himself or another person, or (ii) cause loss to the data subject. It is also an offence if the unauthorised disclosure, irrespective of its intent, causes psychological harm to the data subject. The maximum penalty for these new offences is a fine of $1,000,000 and imprisonment for 5 years.

[2] DPP4 (1) requires that all practicable steps should be taken to ensure that personal data held by a data user are protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to – (a) the kind of data and the harm that could result if any of the security incidents should occur; (b) the physical location where the data is stored; (c) any security measures incorporated

of the PDPO to take all reasonably practicable steps to ensure that personal data stored in the System is protected against unauthorised or accidental access, processing, erasure, loss or use. It is noted that a prescribed healthcare provider is explicitly required (under section 35 of the Bill) to ensure that its own electronic medical record system does not impair the security or compromise the integrity of the System. Apparently, safe operation of the electronic medical record systems of the prescribed healthcare providers may affect the System security as a whole. To comply with DPP4, effective monitoring of these systems by the eHRC is important. However, with the special immunity provided under section 57(2), even if the eHRC had failed to comply with DPP4, he may refuse to follow the PCPD's directive to tighten up monitoring the healthcare providers' electronic medical record systems through regular or periodic inspections.

22. This diminished role of the eHRC in ensuring the security of the System is in sharp contrast to the role of the HA in managing public hospitals in Hong Kong, including the setting up of policies and guidelines for adoption by public hospitals in the protection of patients' personal data, and ensuring compliance through inspections and other audit work.

23. Thirdly, each and every data user is obliged under DPP2(1) in Schedule 1 of the PDPO to take all reasonably practicable steps to ensure the personal data it collects, holds, processes and uses is accurate having regard to the purpose for which the personal data is used or is to be used[3]. Even though

---

into the equipment for data storage; (d) any measure taken for ensuring the integrity, prudence and competence of persons having access to the data; and (e) any measures taken for ensuring the secure transmission of the data.

[3] DPP2(1) requires that,

(1) All practicable steps shall be taken to ensure that-

(a) personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;

(b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used-

(i) the data is not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data is erased;

(c) where it is practicable in all the circumstances of the case to know that-

(i) personal data disclosed on or after the appointed day to a third party is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and

the healthcare recipients' eHR data is supplied by registered healthcare providers, the PCPD finds the proposed exoneration of the responsibility to inspect for data accuracy odd, since data accuracy is the cornerstone for the patients' healthcare and the effectiveness of the System.

24. A close analogy to the eHRC is a credit reference agency that collects individuals' consumer credit data from credit providers and maintains a centralized database for the provision of consumer credit data to credit providers to facilitate their assessment of applications for loans and other credit facilities. This is subject to regulation under DPP2(1) (governing data accuracy) and the *Code of Practice on Consumer Credit Data* published by the PCPD[4]. The credit reference agency is not exonerated of its obligations as a data user under DPP2(1) in any way.

25. For reference, under the Australia's Personally Controlled Electronic Health Records Act 2012, the system operator of personally controlled eHR in Australia, which performs similar functions as the eHRC, is not offered any such exclusion from inspection[5].

Concluding Remarks

26. Operation of the System involves the uploading, storing and sharing of massive sensitive health-related data. The PCPD urges the Administration to consider the above comments that are made with a view to safeguarding personal data privacy protection with a robust legal framework and administrative infrastructure at a level no less than that provided under the PDPO and commensurate with the privacy and sensitivity of the health data involved.

(ii) that data was inaccurate at the time of such disclosure, that the third party-
(A) is informed that the data is inaccurate; and
(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

[4] See link to the Code of Practice on Consumer Credit Data published in the PCPD's website: http://www.pcpd.org.hk/english/publications/files/CCDCode_2013_e.pdf

[5] Reference can be made to sections 11 to 12 and Part 5 of the Personally Controlled Electronic Health Records Act 2012 (http://www.comlaw.gov.au/Details/C2012A00063).

27. The PCPD is represented at the Administration's Working Group on Legal, Privacy and Security Issues of the System and has been providing comments on privacy matters. To a large extent, the comments explained above have been conveyed to the Administration. To avoid any conflict of its enforcement role, the PCPD will cease to act as a member of any future standing committee that may be set up upon commencement of operation of the System, although he is prepared to provide further comments on an *ad hoc* basis.

28. Finally, the PCPD would like to be updated on the timing of implementation of the System and expects that sufficient resources would be allocated to his office to support the associated complaint handling and enforcement work.

The Office of the Privacy Commissioner for Personal Data
21 May 2014