Our Ref.: PCPD(O) 25/145/55 Pt. 2

(By Fax : 2102 2525 and By Post)

13 June 2008

Secretary for Food and Health
Food and Health Bureau
19/F., Murray Building
Garden Road
Central, Hong Kong

Dear Sir,

Healthcare Reform Consultation Document
Issued in March 2008

On behalf of the Privacy Commissioner for Personal Data (the "**Commissioner**"), I write to provide our comments on your Healthcare Reform Consultation Document from our perspective as the regulator of the Personal Data (Privacy) Ordinance (the "**Ordinance**").

Our Comments

2. Chapter 4 of your consultation document proposes to establish an electronic health record sharing system (the "**System**") with a view to enabling healthcare professionals in both public and private sectors to enter, store and retrieve patients' medical records.

3. Medical records of living individuals are "personal data" as defined under section 2(1) of the Ordinance. Hence any proposal to establish a computer system containing patients' medical records warrants careful thought in terms of the potential impact that such system would have upon the data privacy rights enshrined in Data Protection Principle ("**DPP**") 1 to DPP6 in Schedule 1 to the Ordinance.

DPP1: Data Collection Principle

4. You should ensure that no excessive personal data are collected having regard to its operating purpose. Where personal data are collected from data subjects, you should communicate to the data subjects the prescribed information under DPP1, including the purpose for collecting the data and the classes of transferees of the data.

DPP2: Data Quality and Retention Principle

5. You should take all reasonably practicable steps to ensure that records kept in the System are accurate. Where the personal data kept in the System are no longer required, they should be permanently erased unless retention is permitted by law.

DPP3: Use Limitation Principle

6. Given that certain medical diagnoses (e.g. mental abnormalities, AIDS, etc.) are extremely sensitive data, consideration should be given to limiting the sharing of particular personal data and the class of transferees.

DPP4: Data Security Principle

7. In view of the sensitive nature of medical records stored in the System and the potentially large number of users of the System, the security features of the System are therefore of particular importance.

8. You should implement reasonable and sufficient security safeguards to protect the data held by you from unauthorized or accidental access, processing and use having regard to the harm that could result, and take steps to guard against any "function creep" in using or comparing the data collected for other purposes.

9. You may consider using a safer framework for the System to ensure secure data transmission on the Internet (e.g. Virtual Private Network) and

impose contractual obligations on service providers to deter unauthorized or accidental access to the System.

DPP5: Transparency Principle

10. You should promulgate and communicate your policy and practice on personal data management in relation to the operation of the System. To comply with DPP5 and alleviate individuals' personal data privacy concern, you should make your privacy policy statement available for public access.

DPP6: Access and Correction Rights

11. Data subjects should be able to exercise their rights to access and correct the information about them that are collected by you and held by the System.

Privacy Impact Assessment ("**PIA**")

12. As the implementation of the System will impact upon the collection, use and sharing of personal data, we strongly recommend that a PIA be carried out so as to identify any actual or potential effects that the System may have on privacy. PIA helps a data user determine how a technological project involving personal data be proceeded.

13. Though the carrying out of a PIA is not a statutory requirement under the Ordinance, we consider that the process of a PIA is a valuable technique for you to assess privacy risks arising from the System, thereby enabling you to reduce or mitigate any adverse effects.

Privacy Compliance Audit ("**PCA**")

14. We also consider it important that PCA on the System be conducted regularly after implementation of the System to ensure the compliance of data protection requirements and prevention of abuse of data collected.

15. In essence, PCA in relation to a personal data system is a systematic verification of compliance with privacy policies, data protection principles, code of practice or other regulatory requirements with respect to information handling and privacy.

16. Consideration should be given to incorporating an audit requirement as a provision in a code of practice that governs the System. This approach has the benefit that rules on the collection, use and access of patients' data can be developed in parallel with the implementation of the System and in tandem with the development in technology.

Code of Practice ("**COP**")

17. You may consider drawing up a COP in consultation with the Commissioner after completion of the PIA study. The COP should set out the ground rules on the collection, use of and access to patients' data and the conduct of PCA. The COP may be covered by section 12 of the Ordinance.

18. Section 12(1) of the Ordinance empowers the Commissioner to issue COP for the purpose of providing practical guidance in respect of any requirements under this Ordinance imposed on data users. For example, the Commissioner has issued a "Code of Practice on Consumer Credit Data" for protecting privacy of individuals in relation to their credit data. This code governs the collection, accuracy, use, security, access and correction of such data by credit reference agencies and credit providers.

Hong Kong Identity Card ("**HKIC**")

19. HKIC numbers are commonly collected and used by data users in Hong Kong to identify individuals and manage records relating to them. However, the indiscriminate use of HKIC numbers may unduly infringe the privacy of the individuals, besides creating opportunities for fraud.

20. It is our view that while HKIC numbers will continue to be used for authentication purpose, you may consider allocating a unique identification

number to each patient in your new centralized electronic health record system. The creation of a unique patient's number may alleviate the heavy reliance on a patient's HKIC number, thereby minimizing the harm that would result in the event of an accidental leakage of patients' medical records.

Conclusion

21. In conclusion, we take the view that sufficient privacy safeguards must be in place when designing the System, in particular :

(a) collecting only a minimum amount of data needed to serve the purpose of electronic health record sharing;

(b) ensuring data subjects fully understand (i) the purpose of collection of their data and (ii) the purpose of sharing their data through the System by effective communication through different media; and

(c) ensuring minimum harm is caused to data subjects in the event of data leakage (e.g. illegal hacking and the like).

22. The above sets out our views on your consultation document. Should you have any queries, please feel free to contact the undersigned at 2877 7173.

Yours faithfully,

(Allen TING)
Acting Chief Privacy Compliance Officer
For Privacy Commissioner for Personal Data