香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Our Ref.: PCPD(O)25/25/161/215 pt.1

16 March 2015

(By Fax (2102 2525) & By Post)

Secretary for Food and Health Bureau
Healthcare Planning and Development Office
Food and Health Bureau
19/F, East Wing
Central Government Offices
2 Tim Mei Avenue, Tamar
Hong Kong

Dear Sirs,

Public Consultation on Regulation of Private Healthcare Facilities

We refer to the captioned public consultation and send herewith the Submission from our office for your attention.

If you have any questions, please feel free to contact the undersigned or our Mr Leung at .

Yours faithfully,

(Sandra LIU)
Senior Legal Counsel
for Privacy Commissioner for Personal Data

Encl.

香港灣仔皇后大道東 248 號陽光中心 12 樓 12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852)2827 2827 傳真 Fax (852)2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

PCPD's Submissions in response to Public Consultation on Regulation of Private Healthcare Facilities

This submission is made by the Office of the Privacy Commissioner for Personal Data ("**PCPD**") in response to the Public Consultation ("**Consultation Document**") carried out by the Food and Health Bureau ("**FHB**") on the Regulation of Private Healthcare Facilities ("**PHFs**") respectively. As the regulator to protect individuals' privacy in relation to personal data under the Personal Data (Privacy) Ordinance (Cap.486) ("**Ordinance**"), the PCPD would like to raise concerns on some of the proposals from the perspective of personal data privacy protection.

2. Coupled with the proposed Voluntary Health Insurance Scheme ("**VHIS**")[1], the Administration considered that there is a genuine need to revamp and modernise the regulatory regime for PHFs in view of the advancement in medical technology and practices. Public views are sought on the proposed (i) classification of PHFs, (ii) regulatory requirements, and (iii) regulatory authority. With the personal data of patients in mind, the PCPD would address the latter two proposals.

Regulatory Requirements

A. Corporate Governance

(A4) Establishment of an Information System Connectable with the Electronic Health Records System Scheme

[1] The PCPD has also made Submissions on the Public Consultation on VHIS (which is available at PCPD's website).

3. It is proposed that hospitals should develop an internal electronic medical patient record system that meets the technical requirements to be connectable with the territory-wide and patient-oriented Electronic Health Records System Scheme ("**eHRSS**"). This regulatory requirement is proposed, for the time being, not to apply to non-hospital PHFs (see paragraphs 5.27 to 5.28 of the Consultation Document). The ultimate purpose is to enhance better access and sharing of patients' health records (with their consent) for smooth transition of patients between different levels of care as provided in the public and private healthcare sectors.

4. Regarding the setting up of the eHRSS, the PCPD has already provided comments on the proposed eHRSS Bill[2] and the infrastructure of the future eHRSS[3]. Currently, the Legislative Council Bills Committee is still vetting the eHRSS Bill which regulates the sharing of patients' health records.

5. In establishing hospitals' internal electronic systems, the Administration must adopt measures to ensure hospitals develop not only the required technical designs for system security but also clear policies and practices for handling data breach and governing access to and use of patients' health records. Such internal systems must be designed to incorporate the privacy features under the eHRSS and align with the *patient's consent* and *need-to-know* guiding principles. For example, only healthcare professionals providing healthcare to the patients should be given access to the data (stored in the PHFs' respective internal systems) which may be relevant to the healthcare provided at the material time. System logs or audit trials should be built in to trace the access by individual healthcare professionals.

---

[2] See the eHRSS Bill from the Legislative Council's website (http://www.legco.gov.hk/yr13-14/english/bills/b201404172.pdf).

[3] For details, please refer to the PCPD's Submission in response to the "*The Legal, Privacy and Security Framework for Electronic Health Record Sharing*" (available at http://www.pcpd.org.hk/english/enforcement/response/files/eHR20120210.pdf) and the PCPD's Submission on the eHRSS Bill (available at http://www.pcpd.org.hk/english/news_events/media_statements/files/eHR_legco_paper_e.pdf).

Embrace Personal Data Privacy Protection

6. Apart from the five regulatory aspects (A1 to A5 as mentioned in the Consultation Document), the PCPD advocates that the PHFs (as organisational data users) should also embrace personal data privacy protection as part of their corporate governance responsibilities. The PHFs collect, hold, process and use vast amount of personal data during their encounters with patients, including in particular health data which is inherently sensitive. To manage privacy and data protection responsibly and to demonstrate their commitments to good corporate governance, the PHFs should adopt a proactive strategy by formulating and implementing a comprehensive privacy management programme ("**PMP**").

7. PMP serves as a strategic framework to assist an organisation in building a robust privacy infrastructure and service designs supported by on-going review and monitoring process to facilitate compliance with the requirements under the Ordinance[4]. It involves top management commitment and ensures that privacy is built by design into all initiatives, programmes and services.

8. As part of the PMP, the PHFs should establish a procedure for managing personal data breach incidents (e.g. data leakage), including a system of notification. While reporting of a data breach to the PCPD is not a mandatory requirement under the Ordinance, the PHFs should be encouraged to adopt a system of notification of these data breach incidents (to be given to the affected data subjects, the PCPD and/or the regulatory authority (if applicable) as well

[4] The detailed guidelines can be found in the PCPD's "*Best Practice Guide on Privacy Management Programme*" (available at http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/PMP_guide_e.pdf).

as the law enforcement agencies (if appropriate))[5]. This voluntary notification is an existing practice of public hospitals.

9. Another essential part of the PMP is that its effectiveness should be monitored and reviewed regularly. As part of good corporate governance, the PHFs should consider conducting privacy compliance audit for the purposes of assessing and evaluating the level of privacy compliance with the Ordinance, identifying potential weaknesses in the data protection system and providing recommendations for improvement of the system.

C. Clinical Quality

(C9) Service Delivery and Care Process

Policy to Protect Patients' Privacy

10. It is noted that the Administration proposed to revamp the quality of medical services provided by the PHFs. The PCPD is pleased to note that two of the proposed regulatory standards for service delivery and care process cover the protection of patients' medical records and privacy[6]. In gist, the PHFs are required to formulate policies to manage medical records and protect patients' privacy in compliance with the regulatory standards in the form of regulations or codes of practices issued by the regulatory authority governing the PHFs (see paragraphs 7.9(c) and (d) and 10.6 of the Consultation Document).

---

[5] See the "*Guidance on Data Breach Handling and the Giving of Data Breach Notifications*" issued by the PCPD (available at http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/DataBreachHandling_e.pdf) which provides practical guidance in this regard.

[6] According to paragraph 7.9 of the Consultation Document, it is proposed that the regulatory standards include *"(c) a properly managed medical record system to ensure all medical records are accurate and up-to-date and are kept in a secure and confidential manner; (d) policy to protect patients' rights such as privacy, confidentiality of their medical records, informed consent before medical intervention, and a safe care environment"*.

11. To ensure that patients' rights to personal data privacy are duly protected, it is submitted that the internal policies of the PHFs should cover detailed practices and procedures involving the collection, retention and use of patients' personal data, the security measures adopted to safeguard the data and patients' rights to access to and correction of their data. From the PCPD's regulatory experience, there are often disputes between patients and medical practitioners in relation to the data access requests and the fees charged by the medical practitioners for complying with such requests as well as the accuracy of medical opinions. Clear policies in compliance with the Ordinance in these areas should not be overlooked by the PHFs.

12. Further, it remains unclear from the Consultation Document as to the consequence of non-compliance with the PHFs' internal policies, regulations or codes of practices issued by the regulatory authority. The PCPD submits that non-compliance must entail penal consequences so as to achieve the desired deterrent effect. To achieve this end, the regulatory authority must be vested with adequate investigative and enforcement powers. Moreover, proper sanctions should be introduced in the future legislative and administrative frameworks.

E. Sanctions

(E19) Sanctions

13. It is proposed that sanctions should be imposed on the PHFs in ensuring compliance with the proposed regulatory requirements; and these sanctions should be commensurate with the risks involved in the operation of the PHFs (see paragraphs 9.1 and 9.6 of the Consultation Document).

Non-compliance with Regulations or Code of Practices

14. The PCPD submits that the Administration should consider introducing sanctions against non-compliance with the regulations or codes of practices to be issued by the regulatory authority setting out the principles, procedures, guidelines and standards in managing the PHFs (which include protection of patients' privacy as proposed in paragraph 7.9(c) and (d) of the Consultation Document). Consideration should be given to the imposition of fines or suspension/ revocation of PHFs' operating licences. Besides, non-compliance by individual healthcare professionals must be dealt with seriously such as instituting disciplinary proceedings.

Criminal Sanctions

15. Separately, in view of the inherently sensitive nature of medical records, the PCPD invites the Administration to consider the appropriateness to introduce proper offence(s) to deter the unauthorised access or misuse of patients' health records obtained from the PHFs. Under the proposed eHRSS Bill, specific offences are introduced for (i) knowingly causing a computer to perform any function so as to obtain unauthorised access to the data in the eHRSS, and (ii) causing access to the data in the eHRSS with the intent to commit an offence, deceive, make dishonest gain or cause loss to another[7]. The PCPD submits that similar offences should be considered for safeguarding the data kept in the internal systems of PHFs, which will be ultimately made connectable to the eHRSS as proposed.

Powers of Regulatory Authority

16. For effective regulation of the PHFs, the regulatory authority must be vested with adequate powers not only to control the requisite licensing for the

[7] See the offence provisions under Part 5 of the eHRSS Bill.

PHFs but also to conduct inspection and investigation to ensure compliance with the various proposed regulatory requirements. It is noted from paragraphs 10.5 and 10.7 of the Consultation Document that the regulatory authority will indeed be given such regulatory powers.

Disclosure of Confidential Information in Sentinel Events and Medical Incidents

17. It must be pointed out that mishandling of personal data (e.g. identity of the victim(s) of medical incidents, staff of the hospital, etc.) and excessive disclosure of relevant information in reporting/ investigation of the sentinel events/ medical incidents could be highly intrusive upon the privacy of the affected individuals. It may also be prejudicial to the proper conduct of criminal investigation and the ensuing legal proceedings (if any). Therefore, due regard must be given to protect the personal data of the *individuals* affected. Under section 48(3) of the Ordinance, the Privacy Commissioner is required to prevent the disclosure of the identity of individuals in publishing an investigation report. The Administration may consider introducing similar provisions in the future legislative framework for publication of investigation reports without revealing individuals' personal data.

18. On the other hand, it is submitted that the PCPD should be expressly made as an exception to whom confidential information may be disclosed so as to facilitate investigation by the PCPD on potential criminal offences, improper conduct or practices which may amount to contraventions of the requirements under the Ordinance.

Concluding Remarks

19. The Consultation Document put forward broad proposals on the future regulatory regime for the PHFs. The PCPD urges the Government to consider

personal data privacy protection when taking forward the proposals and designing the legislative and administrative frameworks in due course. In this regard, the PCPD would like to be further consulted on any privacy-related issues as they arise.

The Office of the Privacy Commissioner for Personal Data
16 March 2015