PCPD's Submissions in response to Public Consultation on Voluntary Health Insurance Scheme

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 Voluntary Health Insurance Scheme ("**VHIS**"). 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. The VHIS (formerly known as Health Protection Scheme) is intended to regulate individual indemnity hospital insurance policies so as to re-calibrate the dual-track healthcare system currently provided by the public and private healthcare sectors in Hong Kong. Public views are sought on eight questions concerning the institutional framework for implementing the VHIS. The PCPD would like to furnish its views on two specific questions posed therein.

Question: Do you have any particular views on the 12 Minimum Requirements proposed for improving the accessibility, continuity, quality and transparency of individual Hospital Insurance?

Portable Insurance Policy

3. One of the minimum requirements proposed is portable insurance policy. It is proposed that upon implementation of VHIS, all insurers who offer individual hospital insurance products must provide a standard plan (with

essential features) which complies with the proposed minimum requirements[1]. In particular, it is proposed that policyholders should enjoy free portability (i.e. without re-underwriting) as far as possible such that policyholders of insurance products complying with the minimum requirements may transfer their policies to other insurers subject to certain conditions (see paragraph 2.30 of the Consultation Document[2]).

4. At the present stage, the detailed transfer arrangement is not yet certain (for instance, whether a platform will be provided by the Administration). Nevertheless, it is anticipated that when policyholders are permitted to make their own decisions to transfer their policies to other insurers, there will be massive transfer of their personal data[3] (e.g. full name, data of birth, Hong Kong Identification Card numbers, etc.) between insurers. Hence, the requirements (including the Data Protection Principles ("**DPP**") in Schedule 1) under the Ordinance must be observed.

5. In formulating the transfer mechanism, one of the cardinal principles is that personal data to be transferred should be limited to the extent necessary for the purpose of the transfer. Excessive disclosure of personal data may amount to a change in the purpose of use (which includes "transfer" or "disclose" as defined under the Ordinance) of the data[4].

---

[1] According to paragraph 2.19 of the Consultation Document, the 12 proposed minimum requirements are the standards to be met by the insurance policies under the VHIS. It can be grouped into three categories, namely (a) improving accessibility to and continuity of insurance, (b) enhancing quality of insurance protection, and (c) promoting transparency and certainty. An individual hospital insurance that meets all (but not exceeding the minimum requirements) is considered as Standard Plan/ compliant policies.

[2] According to paragraph 2.30 of the Consultation Document, "Portable Insurance Policy" is one of the 12 proposed minimum requirements for individual health insurance policies. The aim is to enable policyholders to enjoy free portability (i.e. without re-underwriting) as far as possible for enhancing consumer choice and promoting healthy competition among insurers.

[3] Section 2(1) of the Ordinance stipulated that "*personal data*" means "*any data relating directly or indirectly to a living individual from which it is reasonable practicable for the identity of the individual to be directly or indirectly ascertained and in a form in which access to or processing of the data is practicable.*"

[4] See DPP 3(1) of the Ordinance.

6. In addition, the PCPD is concerned with the security of personal data stored or transmitted in the proposed transfer arrangement. Although the details of the arrangement have yet to be formulated, one must bear in mind that all reasonably practicable steps must be taken to ensure the personal data is protected against unauthorised or accidental access, processing, erasure, loss or use[5]. It is necessary to consider, among others, the kind of data concerned and the harm that could result if the data is not securely kept.

7. For instance, appropriate security measures may include a secure IT framework for the transmission of data (e.g. with proper encryption to avoid unauthorised access or the adverse effects of data leakage), a secure IT computer network for storage and processing of data (e.g. with up-to-date software enabling password-control and encryption) and other measures to ensure safe custody of the personal data contained therein.

8. The regulatory agency to be set up should devise detailed data handling policies and procedures covering the aforesaid aspects and advise on the appropriate security measures to be adopted to protect the personal data to be transferred.

Question: Do you support establishing a regulatory agency under the FHB to supervise the implementation and operation of the VHIS; and a claims dispute resolution mechanism for resolving claims disputes under the VHIS[6]?

9. It is proposed that a regulatory agency shall be set up under the FHB to supervise the operation of the VHIS. The proposed regulatory agency will

[5] See DPP 4(1) of the Ordinance.

[6] Regarding the latter half of this question, it is noted that a claims dispute resolution mechanism will be established to provide a credible and independent channel alternative to litigation for resolving claims disputes under the VHIS (paragraphs 6.15-6.27 of the Consultation Document). Since the proposed mechanism does not relate to the information systems and other facets of personal data collection, the PCPD does not provide any views in this regard.

perform a host of functions that are regulatory or facilitating in nature. One of the facilitating functions is to develop information systems for product filing, data collection and publishing of data from insurers and healthcare providers (see paragraphs 6.5 and 6.6 of the Consultation Document). In addition, the regulatory agency shall collect, collate and analyse data which is necessary for the regulators, consumers and the industry to, among others, enhance transparency and provide necessary information for successful implementation of Diagnosis-related Groups (DRG)-based packaged pricing[7]. This process is expected to continue for a prolonged period of time (see paragraph 2.43 of the Consultation Document[8]).

10. The PCPD is particularly concerned with the design of the information systems, which will be established and operated by the regulatory agency. Given that an extensive amount of data will be involved (ranging from policy details, information on applicants recommended for admission to the High Risk Pool, etc.[9]), it is incumbent upon the relevant data users (which can be the insurers, the healthcare providers or the regulatory agency depending on the circumstances) to notify the individuals of the above purposes of use of their personal data, the classes of transferees, etc. on or before the collection of individuals' personal data[10].

11. Further, it is noted that the proposed regulatory agency shall have broad authority to, among others, prescribe the form for data taking[11]. The PCPD stresses that only adequate but not excessive personal data which is

[7] See the section on "*Data Collection*" on page 168 of the executive summary of the consultancy study at Appendix C (pages 147-177).

[8] According to paragraph 2.43 of the Consultation Document, it is considered that "*it would take a relatively longer time for Hong Kong to develop an operable system of DRG suitable for local use in the private sector. The exercise would require comprehensive and regular collection, compilation and analysis of healthcare, claims and pricing data from the health insurance industry and healthcare providers. Regular and structural review is also required to keep the DRG system up-to-date*."

[9] The 16 categories of information to be collected from insurers and healthcare providers are found in "*Table 5: Overview of Data Collection Strategy*" on page 169 of the executive summary of the consultancy report at Appendix C (pages 147-177).

[10] See DPP 1(3) of the Ordinance.

[11] See the section on "*Data Collection*" on page 168 of the executive summary of the consultancy study at Appendix C (pages 147-177).

necessary for achieving the function and activity of the relevant data users shall be collected[12]. The regulatory agency should pay heed to the extent and the types of personal data to be collected.

12. In particular, the PCPD stresses that even though the raw data itself may have been anonymised[13] by the insurers and healthcare providers before they are provided to the regulatory agency for further processing and reporting[14], the identity of a particular individual may well be "re-identified". In other words, there are limits to anonymisation of data. This may be illustrated with a classic incident that occurred in the US.

13. In mid-1990s, the Massachusetts Group Insurance Commission decided to release anonymised data on state employees' medical records for research purpose. The medical record showed all hospital visit(s) made by each of the state employees with all personal identifiers (e.g. full name, address and Social Security numbers) removed. However, a graduate student was able to "re-identify" certain individuals with a voter database. This happens way before the computer age where personal information was readily gathered by various means[15]. A recent research even revealed that the risks of re-identifying people from anonymised sensitive data may be as high as 87% even for simple demographic data[16]. Hence, the Administration should address the potential risks associated with the collecting, processing and reporting of raw data by the regulatory agency.

---

[12] See DPP 1(1) of the Ordinance.

[13] The 16 categories of information to be collected from insurers and healthcare providers as listed in "*Table 5: Overview of Data Collection Strategy*" may include premiums by age band for HPS Standard plans, inpatient activity data reported using a standardised terminology, demographic data on patients using the services.

[14] See the details on reporting to consumers, industry and policymakers in "*Table 6: Overview of Reporting Framework"* on page 169 of the executive summary of the consultancy report at Appendix C (pages 147-177).

[15] Details of the Massachusetts state employees' medical records incident may be found at: http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/.

[16] See the research made by L. Sweeney, *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University (available at http://dataprivacylab.org/projects/identifiability/paper1.pdf).

Adopt Privacy Impact Assessment in Devising Measures to Implement VHIS

14. It would be premature to provide further comments as the aforesaid proposals are still in their infancy. Suffice it to say that due consideration must be given in handling such sensitive data involving a significant population in Hong Kong. The PCPD suggests that a Privacy Impact Assessment ("**PIA**")[17] should be conducted to identify the potential risks inherent in the information systems which affect individuals' personal data privacy in the whole data cycle.

15. Although not a statutory requirement, PIA is a valuable tool to systematically assess the privacy risks associated with the design of the data collection mechanism, thereby mitigating any risks of encroaching on the privacy rights of individuals. Further, a *privacy-by-design* approach should be adopted to incorporate privacy protection into the new scheme from the design stage to its implementation.

Outsourcing of Personal Data

16. It is noted that the regulatory agency may outsource the tasks of collecting, collating and processing of data to other organisations[18] as data processors[19]. In the circumstances, it must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data[20]; and to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor[21].

---

[17] For details of the PIA, please refer to the "*Information Leaflet on Privacy Impact Assessments*" issued by the PCPD (available at: http://www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/files/PIAleaflet_e.pdf).

[18] See the section on "*Data Collection*" on page 169 of the executive summary of the consultancy study at Appendix C (pages 147-177).

[19] "*Data processor*" means "*a person who (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes*."

[20] See DPP 2(3) of the Ordinance.

[21] See DPP 4(2) of the Ordinance.

17. Owing to the inherently sensitive nature of the data, mishandling (or leakage) of the data will be highly intrusive to the patients. Therefore, it would be prudent for the regulatory agency to enter into contractual arrangements with its data processor(s) to protect the relevant personal data. If the data processor's act or practice contravenes the requirements of the Ordinance, the regulatory agency will be ultimately responsible as a principal for the act of its agent[22]. In this connection, the PCPD has issued an "*Information Leaflet on Outsourcing the Processing of Personal Data to Data Processors*"[23] to provide guidance on a data users' obligations and suggest typical contractual obligations that may be imposed on the data processors.

18. If the proposed outsourcing will be made to an overseas data processor or that the personal data will be transferred to a place outside Hong Kong by the data processor, due consideration must be given to section 33 of the Ordinance (on prohibition against cross-border data transfer except under prescribed conditions). The purpose of such cross-border data transfer restriction is to ensure that the transferred personal data will be afforded a level of protection comparable to that under the Ordinance. Although section 33 of the Ordinance is not yet effective, it is prudent to follow the guidance provided by the PCPD[24].

Concluding Remarks

19. The Consultation Document put forward broad proposals governing the future implementation of the VHIS. The PCPD urges the Government to

[22] Section 65(2) of the Ordinance stipulated that "*any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of this Ordinance as done or engaged in by that other person as well as by him*."

[23] The Information Leaflet is available at: http://www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/files/dataprocessors_e.pdf.

[24] See PCPD's "*Guidance on Personal Data Protection in Cross-border Data Transfer*" (available at: http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf).

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