Comments on the Public Consultation Document for the Legal, Privacy and Security Framework for Electronic Health Record Framework

The Electronic Health Record (eHR) Sharing System will give timely access and sharing of participating patients' health data to authorised healthcare providers in both public and private sectors. In our view, data privacy and system security are the most important cornerstones that underpin the development and implementation of such a system.

The Office of the Privacy Commissioner for Personal Data ("PCPD") has considered the Consultation Document for the Legal, Privacy and Security Framework for Electronic Health Record Framework ("the Consultation Document") from the policy, legal and compliance perspectives of the Personal Data (Privacy) Ordinance ("the PD(P)O"). We have pleasure in setting out our submissions below.

Supportive views:

1. <u>Electronic Health Record ("eHR") specific legislation and measures</u>

1.1 PCPD welcomes and supports the proposition that specific legislation for governing the eHR Sharing System is needed to complement and supplement the PD(P)O [paragraph 3.7]. This will lay down the basis for the operation of the eHR Sharing System, and give legal recognition to health records as a type of sensitive personal data that deserve greater protection by the introduction of specific legislation.

1.2 PCPD supports the principle that participation in the eHR Sharing System is voluntary and only after express and informed consent has been given by patients [paragraph 4.4.a]. This is in line with Data Protection Principle ("DPP") 3 of the PD(P)O which requires that data subject's prescribed consent is to be given.

1.3 PCPD supports the principle of limiting the sharing of eHR data to those healthcare providers as is necessary for the delivery of care for the patients and with their consent [paragraph 4.4.b] under the proposed "patient-under-care" and "need-to-know" principles.

1.4 PCPD welcomes the eHR office to follow prudent privacy protection

measures such as conducting privacy impact assessment[1], privacy compliance audit[2], security risk assessment[3] and security audit[4] to ensure compliance with the relevant legislative requirements.

Legal, policy and compliance views:

2. The role of the Code of Practice (COP)

2.1 Under paragraph 22 of the Executive Summary, and paragraphs 3.18 and 4.50 of the Consultation Document, a COP will be developed to bind healthcare providers on how they and their electronic medical/patient record ("eMR/ePR") systems would operate. However, the Consultation Document has not addressed how the eHR Sharing System operating body ("eHR-OB") itself and the eHR Sharing System will be governed. As a number of responsibilities have been identified in the Consultation Document to be given to the eHR-OB, such as on complaint and review mechanism on the access and use of eHR data [paragraph 4.47], the use of non-patient identifiable data [paragraph 4.38], and data access request ("DAR")/data correction request ("DCR") arrangements [paragraph 4.44], the legislation should consider also mandating a COP to be developed on the governance of the eHR-OB and the eHR Sharing System (in areas such as internal access, control, security, audit and breach notification requirements) in a transparent manner to better instil public confidence.

2.2 Furthermore, the effectiveness of the COP is called into question when there is no explicit stipulation of the punitive consequence on breaching the COP [paragraph 4.50]. There should be a clear legal consequence or penalty on the contravention of the COP. Although the proposed legislation may address the complaint and review mechanism in relation to the eHR Sharing System, it is

[1] A privacy impact assessment is generally regarded as a systematic risk assessment tool that can be usefully integrated into a decision-making process. It is a systematic process that evaluates a proposal in terms of its impact upon personal data privacy with the objective of avoiding or minimising adverse impact.

[2] The privacy compliance audit aims at (i) assessing and evaluating the level of privacy compliance with the PDPO, in particular the six Data Protection Principles in Schedule 1 to PDPO, with respect to the collection, processing and handling of personal data; (ii) identifying potential weaknesses in the data protection system; and (iii) providing recommendations for a review of the data protection system.

[3] Security Risk Assessment can be defined as a process of evaluating security risks, which are related to the use of information technology. It can be used as a baseline for showing the amount of change since the last assessment, and how much more changes are required in order to meet the security requirements.

[4] Security Audit is a process or event with the security policy or standards as a basis to determine the overall state of the existing protection and to verify whether the existing protection has been performed properly. It targets at finding out whether the current environment is securely protected in accordance with the defined security policy.

important that both the legislation and the COP should not take precedence or otherwise erode the general power on personal data protection vested in the Privacy Commissioner for Personal Data by the PD(P)O.

3 Voluntary participation, choice and consent

Voluntary participation to the eHR scheme

3.1 The eHR-OB should provide sufficient information to patients, before their enrolment, through the Patient Information Notice [paragraph 4.8], namely: (1) what data will be shared, (2) use of the data (e.g. primary and secondary use), (3) to and with whom the data will be shared (e.g. referral), (4) retention period and (5) patients' data access and correction rights. To ensure that patients are fully informed before giving their consent, they should be informed participation in the scheme is voluntary, and the consequences of not joining the eHR scheme [paragraph 4.4a].

3.2. eHR-OB should also ensure that any existing arrangements or practices on the sharing of health-related data (or equivalent) should still be available to those data subjects who choose not to join the eHR scheme [paragraph 4.4a].

3.3 Since application for enrolment may be made by mail or fax, proper safeguards should be in place to verify the identity of the prospective participant and the veracity of the application [paragraph 4.6].

Safe deposit box and choice

3.4 There is insufficient justification for not implementing the "safe deposit box" in the Consultation Document [paragraphs 4.28 to 4.30]. At present, patients have the choice and discretion whether and what to inform their doctors. We question if the justifications to take away this right are sufficiently valid: the primary argument put forward is that "while recognising the sensitivity of some health data which would warrant extra safeguards, there is a need to balance extra protection for this sensitive data with the completeness and integrity of the eHR to ensure the quality of healthcare delivery." There is, for example, no empirical data (direct or otherwise) or statistics to suggest the presence of a "safe deposit box" will jeopardise the safety of patients. If the justification is that medical professionals require a full picture of the medical history of patient to ensure proper medical service, the patient's consent to access information in the "safe deposit box" should be obtained after

explaining to the patient the relevance and importance of such disclosure. In any event, there is already an existing proposal to allow medical professional access to eHR data in emergency situations where patient's consent cannot be obtained [paragraph 4.19].

The "open-ended" and "one-year rolling" consent models

3.5 Patients should be informed of the practical difference between "open-ended" and "one-year" rolling consent on or before enrolment in the eHR Sharing System [paragraph 4.10]. Patients should also have the means to check, at any time, what types of consent they have given to which healthcare providers.

3.6 The justification for giving "open-ended" access consent alone to Hospital Authority ("HA") and Department of Health ("DH") is unclear [paragraph 4.14]. Under the scheme, it is integral to the registration that patients have to give "open-ended" (but not "one-year rolling") consent for HA and DH to access/upload patients' data. Whilst it may be understandable that HA or DH should be given consent to upload their data to constitute a complete eHR record, there seems to be insufficient justification as to why HA and DH will be treated differently from other healthcare providers with regard to the duration of patients' consent for accessing their data. In particular, if a data subject after being fully informed, chooses to give a "one-year rolling" consent to all other healthcare providers to upload and access data, it is unclear why HA and DH will have to be given an "open-ended" access consent regardless.

Access of eHR records by some sectors of the healthcare providers e.g. allied healthcare providers

3.7 It is not entirely clear if the eHR Sharing System separate the consent to upload data and the consent to access data [paragraph 4.6], given there may be healthcare providers, in particularly those that supply laboratory and radiology results, whose needs to access the entire health records of individuals may not be necessary. Elaboration on whether it is feasible to separate consent for the uploading and consent for the access should be provided.

Case-by-case consent for referrals

3.8 Given the sensitive nature of health data, patients should be given more

information about the identities of the transferees (referred providers) before their health data are transferred. Since the patient information notice regarding the referral arrangement is given at the initial stage, i.e. when the patients enrol in the eHR Sharing System, it is unlikely that the patients would know the identity of the referred providers. It is advisable that patients be allowed to signify their consent before the referral of health information on a case-by-case basis [paragraph 4.15].

Revalidating consent

3.9 Patients will have the option to revalidate their consent to join the eHR programme within a period of three years from withdrawal. However, it is not clear from the Consultation Document whether patients who re-enrol in the eHR Sharing System within three years of withdrawal are allowed to revalidate each previously given consent individually. In order to ensure the effectiveness and completeness of the revalidation, patients seeking to revalidate their consent should be given an exhaustive list of providers to whom they had previously given consent to and individual revalidation allowed.

4 Data Access Request ("DAR") and Data Correction Request ("DCR")

DAR

4.1 The Consultation Document proposes that only a limited scope of the substitute decision makers ("SDMs") be given data access rights. They are persons with parental responsibility over minors and guardians of mentally incapacitated persons ("MIPs") [paragraph 4.42]. Under the PD(P)O, a person with a patient's written authorisation is also permitted to access the data of the patient as his "relevant person"[5]. However such person will not be given the data access right under the proposal. In this regard, the proposal seems to be inconsistent with the general access right under the PD(P)O, and will curtail a patient's right to authorise others to access their data on their behalf. Especially for elderly patients (who are not incapacitated as such), there appears insufficient justification in the Consultation Document why their rights to authorise third parties should be denied.

4.2 Furthermore, it is noted that the Consultation Document proposes that a

[5] Under the PD(P)O, persons with parental control, persons appointed by a court to manage the affairs of persons incapable of managing his own affairs and persons with patients' written authorizations are permitted to access the data of the patient as "relevant persons".

wider scope of SDM, including "immediate family members," will be allowed to give consent for an individual to join the eHR Sharing System [paragraph 4.11]. It is not obvious why patients are allowed to authorise their "immediate family members" [paragraph 4.11] under the eHR framework to grant consent but not to access their data by the same "immediate family members", who have the separate written authorization from the patients[6] to access their data. The justification that the eHR sharing system, as an electronic platform, would not be able to verify the patients' authorisation to a third party [paragraph 4.42] needs further elaboration, as some of such authorised third parties (e.g. immediate family members) will be given the right to join the scheme for the patients. In any event, the eHR system will have to verify their relationship with the patients before they are allowed to give consent on their behalf. It appears that the same verification could be implemented to facilitate access to data.

4.3 Data access right is essential to data protection. As the proposal is not in line with the PD(P)O, clearer justification on the special arrangement should be provided and debated.

DCR

4.4 It is proposed that the healthcare providers who upload the data will be responsible for complying with patients' data correction rights. According to the PD(P)O, the eHR-OB is also a data user and should be primarily responsible for complying with a DCR. Even with the difficulties suggested in the Consultation Document, eHR-OB must deal with a DCR if a healthcare provider fails or refuses to act, particularly in the case where the healthcare provider does not respond within a certain period of time (40 days in the case of the PD(P)O), or cannot be located/identified, etc. The Consultation Document has not provided a clear role of the eHR-OB in the situation of a DCR.

4.5 Drawing reference from the Code of Practice on Consumer Credit Data issued by the Privacy Commissioner, where Credit Reference Agencies are also collecting credit reference data from Credit Providers for consolidation, the Code of Practice on Consumer Credit Data requires that if the Credit Reference Agencies do not receive any written confirmation or correction of the disputed data within 40 days from the DCR, the Credit Reference Agencies shall delete or amend the record upon

[6] Persons with written authorizations from patients are entitled to access patients' data as "relevant persons" under the PDPO.

expiry of the 40 days. Whilst the circumstances may be different with regard to health data, special consideration should be given to ensure that there is at least a remark or "red flag" against the data under dispute if the data is not amended by the healthcare provider who uploaded the data and the correction requested after a certain period of time.

5 Use of Patient-Identifiable Data

5.1 It is proposed that the Secretary for Food and Health may approve any proposal for the use of patient identifiable eHR data for public health research or disease surveillance on grounds of public interest [paragraph 4.37]. The use of patient-identifiable data other than for the provision of healthcare services to that subject patient should *not* be allowed unless otherwise exempted from PD(P)O. The public interest ground should be consistent with or co-terminous with section 59 of the PD(P)O. It is imperative that the data privacy of the subject patients must be protected at all times.

Other Comments on Specific Issues:

Paragraph	Proposal	PCPD's Comments
19 of Executive Summary	Identification	The eHR-OB should explore minimising the use or storage of HKID card numbers in the system, so as to reduce the damage in case of data breach incidents where individuals' health records together with their HKID card numbers could be leaked to unauthorised parties.
4.9 (f)	Provider's access	Whilst a healthcare provider may access the health data if it "needs" to "for delivery of professional healthcare to the patient", the issue of when such "need" arises may be disputable. A patient who is actively consulting a doctor may expect that the doctor would need to access his health data. If, however, a patient has stopped consulting the doctor for some time, does the doctor have the "need" to "review" the patient's records from time to time? Further elaboration may be required.

Paragraph	Proposal	PCPD's Comments
4.10 & 4.14	Validity of Consent	Since health data will be uploaded from HA and DH as soon as the patients consent, patients should be informed as to the type and nature of the personal data held by HA and DH to be uploaded and shared, before they give their consent to join the eHR sharing.
4.11	Special Consent Arrangement and Substitute Decision Maker ("SDM")	As healthcare professionals in elderly homes may give consent on behalf of patients, detailed guidelines should be provided to them to ensure validity of the consent that they give on the patients' behalf.
4.15-4.17	Referral Arrangement	It is important to make sure that the referral under "e-referral" is case-specific and only confined to facilitating team-oriented healthcare delivery to the patient at the material time. There should be counter-measures to prevent transfer of medical record to other healthcare providers under the pretext of "referral".
4.19	Emergency Access without consent	1. In case the access is subsequently challenged, there should be a proper mechanism and an independent party designated to determine whether the access is justified. 2. Access to a patient's eHR data without his prior consent should not be allowed unless the access is in line with section 59 of PD(P)O.
4.20 - 4.23	Retention of eHR of Withdrawn or Deceased Patients	Whilst it is noted that the retention of eHR data of withdrawn patients is for the purpose of dealing with potential claims by withdrawn patients, the security of the "frozen" data can be an issue. It is not explicitly explained what measures will be in place to guard against unauthorised access of such "frozen", and yet traceable data.

Paragraph	Proposal	PCPD's Comments
4.38	De-identification	Though there may be wider public interest in the use of patient-identifiable her data, eHR-OB should beware that under some circumstances (for example, the presence of certain rare disease combined with a unique treatment given to a patient), anonymisation of patients' data by removing direct identifiers may not satisfactorily reduce the risk of subject identification.
4.43	Fee Charged for DAR	It is proposed that a fee will be charged for making the eHR data available. Currently, under s.28 of the PDPO, a data user is allowed to charge a non-excessive fee for compliance of a DAR. The fee imposed must be "directly related and necessary" for complying with the DAR (see Administrative Appeal Board decision in AAB37/2009).
4.48	Criminal Sanction	The level should commensurate with the penalty level under section 64 of the PD(P)O and the newly proposed offence against disclosure of personal data without the consent of data user under the Personal Data (Privacy) Amendment Bill.
4.49 – 4.50	Code of Practice	It is noted that healthcare providers will be required to design an appropriate role-based access control. But it should be more appropriate for eHR-OB to set a standard based on clinical needs and in consultation with the industry, to ensure uniformity of practice of healthcare providers.
4.59	Restriction on Download	Given the proliferation of data breaches involving health information, the proposed COP should extend its control beyond the downloading of eHR data into portable storage devices including standalone computers.

Paragraph	Proposal	PCPD's Comments
4.61	Access Notification	The notification should identify the relevant date, time and name of the healthcare providers/professionals who access the patients' eHR.

The Office of the Privacy Commissioner for Personal Data
February 2012