LEGISLATIVE COUNCIL

Bills Committee

Electronic Health Record Sharing System Bill

The Privacy Commissioner for Personal Data ("PCPD") reiterates his support for the enactment of a specific legislation to regulate the operation of the Electronic Health Record Sharing System and to provide adequate protection to the health data concerned.

2. The attached table sets out the major concerns of the 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 and the PCPD's comments on the Administration's responses in LC Paper No.CB(2)1775/13-14(02).

Office of the Privacy Commissioner for Personal Data
14 July 2014

Summary of PCPD's Comments and Responses

Glossary

"*DPP*"	-	data protection principle in Schedule 1 of the PDPO
"*eHR*"	-	electronic health record
"*eHRC*"	-	Commissioner for Electronic Health Record
"*HCP*"	-	healthcare provider
"*HCR*"	-	healthcare recipient
"*PDPO*"	-	Personal Data (Privacy) Ordinance (Cap 486)
"*eHRSS*"	-	Electronic Health Record Sharing System

Clause no. of the Bill	The Administration's responses to PCPD's concerns	Summary of PCPD's comments to the Administration's responses
Overall	**eHR-specific legislation's compatibility with the PDPO** • The Administration agreed with the PCPD that the privacy protection offered to HCRs' personal data should be no less than that provided under the PDPO.	• As explained below, there are areas where the PCPD has doubts on whether adequate protection is provided under the Bill.

Clauses 12 to 16 and Clauses 25 to 28	**Sharable scope of data** • The sharable scope of data was drawn up after seeking advice from healthcare professionals, patients groups and IT experts. Patient surveys confirmed it was acceptable to the public and not excessive. In any event, patients will be informed about the sharable scope before they decide whether to join the eHRSS. **Need- to-know principle** • The "*need-to-know*" principle has been adopted in the design of the eHRSS and reflected in the legislative provisions and operation / workflows in the following ways: ➢ Restrictions on use of data are defined in the Bill ➢ An HCR has the choice over granting access only to those HCPs	• The PCPD has no problem with how the scope of data for sharing is delineated for the purpose of provision of healthcare. He is concerned with whether the data will be compartmentalized to enable individual healthcare professionals to gain access to different data compartments on a "*need-to-know*" basis. • Clauses 25 to 28 of the Bill which deal with the permitted use of data and information contained in an eHR are not directly relevant for controlling access to such data and information. • Clauses 12 to 16 of the Bill provide for an HCR to give sharing consent to individual HCPs (hospitals, clinics etc.), not to individual units or personnel of the HCP. In other words, all healthcare professionals of an HCP may gain access to the same set of sharable data relating to the HCR, regardless of their medical disciplines and the nature of healthcare they are providing individually to the HCR. Although a notification (SMS) will be issued by an HCP to an HCR after making access to his eHR, it is doubtful whether the notification will pinpoint the individual healthcare professional who has gained access. • As illustration, the PCPD speculates there are varied clinical needs for the different professionals in each of the following three healthcare groups:

	that have a need to know his health data in the eHRSS. • Only registered healthcare professionals will be granted access to health data in eHR, while administrative staff concerned in an HCP will only be given access to the HCR's index data. ➢ All accesses will be logged and traceable. ➢ Access of an HCR's eHR will trigger the issue of a notification (such as SMS) to the relevant HCR.	➢ Doctor/nurse/physiotherapist/laboratory technician ➢ Dentist/ophthalmologist ➢ Nurse attending emergency care/nurse changing a dressing If affirmative, the justification for them to access the same set of sharing health data would be doubtful. • The PCPD is no expert in such assessment but would expect the Administration to confirm that a professional assessment will indeed be done so that access to the data in eHR will be made by individual healthcare professionals on a truly "*need-to-know*" basis. • To recognise the importance of the cardinal principle that data access will only be made on a "*need-to-know*" basis, the requirement should be expressly spelt out in the Bill.
Overall	**"*Safe deposit box*"** • The Administration recognises the need of some patients to provide enhanced access control to some of their health data due to its high sensitivity but considers that this should be balanced against the completeness and integrity of	• The PCPD strongly supports the "*safe deposit box*" concept as it respects the HCR's right of self-determination of his health data and protects him from discrimination which otherwise could result from inadequate access control of particularly sensitive health data such as psychiatric diseases / mental conditions or hereditary diseases.

	the eHR to ensure the quality of healthcare delivery. • Given these opposing needs and the divergent views gathered during the public consultation in December 2011 to February 2012 and the meeting with the deputations on 26 May 2014, the Administration considers it necessary to conduct an in-depth study before deciding whether to implement a safe deposit box. • The Administration has conducted preliminary desktop researches on overseas experiences (Australia, United Kingdom, Canada and France). None of the overseas experiences is particularly successful to date. • As revealed in a study report published by the World Health Organization	• The requirement for absolute completeness and integrity of the eHR is unrealistic. After all, HCR's participation in the eHRSS is entirely voluntary and the HCP has to attend to his needs and exercise judgment based on the health data it can gather, even if there is no pre-existing eHR because the HCP has not joined the eHRSS. eHR should in any case be used by the HCP as a source of very useful clinical information, not as a substitute for obtaining information from the HCR directly during consultation. • The overriding right of the HCP to open the safe deposit box in emergency situations can be provided for by incorporating suitable exemption clauses in line with section 59(1) of the PDPO[1]. • To address the HCP's concern about liability, it is important that the downside of using the "*safe deposit box*" facility (that is, the lack of full disclosure of health data might affect the quality of the healthcare provided to the HCR) is explained to the HCR. Having made a decision in a well-informed manner, the HCR should assume the responsibility for its consequences. • It was recognized in the WHO report that globally greater patient control of eHR is emerging and it is important that Hong Kong

[1] Under section 59(1) of the PDPO, personal data relating to the physical or mental health of the data subject is exempt from the provisions of DPP3 (governing the use of personal data) in any case in which the application of those provisions to the data would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

	(WHO) in 2012, most countries did not implement options for patients to conceal information in their eHR. Countries are generally concerned that incomplete health records would affect the quality of care and impose liability on management. • The approved budget for implementing the 5-year Stage One eHR Programme does not include a *"safe deposit box"*.	learns from the experiences of countries which have adopted legislation giving patients control over the sharing of their eHR[2]. • It is relevant to note that following a government review of the Personally Controlled Electronic Health Record ("PCEHR") in Australia (in December 2013), it was recommended that the PCEHR should be renamed as My Health Record ("MyHR") retaining all of the patient controls that exist in the current PCEHR (including the right to withhold certain record from being viewed). The review noted that no medical records are complete and that there are some people who legitimately do not want to share everything. Hence the PCEHR should be considered as a source of supplementary information and clinicians should be confident that they will be meeting the appropriate professional standard if they make decisions, in good faith, based on information in the MyHR even if they turn out to be incorrect or incomplete[3]. • The PCPD considers that there has been enough discussion on the subject in the past years and the time is ripe for drawing a conclusion on whether there should be a safe deposit box of some form. He feels that there is no strong opposition from the

[2] See page 61 Report of the World Health Organisation on Legal Framework for eHealth (2012) (available at the link http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf?ua=1)

[3] See page 31 Review of the Personally Controlled Electronic Health Record http://www.health.gov.au/internet/main/publishing.nsf/Content/46FEA5D1ED0660F2CA257CE40017FF7B/$File/FINAL-Review-of-PCEHR-December-2013.pdf

		stakeholders to protecting the patients' right under the eHRSS. Hence further studies and consultation are meaningful only if they are focused on how (instead of whether) to implement the concept. Hong Kong can take a lead in this development instead of waiting indefinitely for the emergence of a best model from other parts of the world. • The PCPD recommends the Administration to (a) incorporate provisions in the Bill to allow for the operation of the safe deposit box and (b) commit to a timetable for working out the details of this facility.
Clauses 17(5)(g) and 20	**Registration as an HCP** • The Administration is prepared to remove Clause 17(5)(g) which allows the registration as an HCP by a specified entity that, in the opinion of the eHRC, directly or indirectly provides healthcare to any HCR. • Clause 20 of the Bill allows the eHRC to register a Government bureau or department as a HCP for the eHRSS if	• The PCPD's concern is how the eHRC will exercise his discretion under the loosely defined situations (under Clauses 17(5)(g) and 20) which would in effect widen the sharing of HCR's eHR. • If the Administration is prepared to remove Clause 17(5)(g), the PCPD sees no point in retaining it. • As regards Clause 20, to avoid unnecessarily widening the discretion of the eHRC, the PCPD suggests that the Administration's policy objectives can be equally met by deleting Clause 20, expanding the definition of *"specified entity"* under

	the eHRC is satisfied that the operation of the bureau or department involves providing healthcare. The Administration quoted as examples of such registrants the Immigration Department or Correctional Services Department as they would also provide healthcare to detainees and may find access to the eHRSS useful.	Clause 17(6) to include Government bureau or department, and requiring these bureau or department to apply for registration under Clause 17(5)(f).
Part 4 and Clause 38	**Disallowing a person authorized in writing by the data subject to make a data access request ("DAR") or data correction request ("DCR") on his behalf** • The proposal is meant to impose stricter control than the PDPO over access of eHR to address concerns regarding possible abuse by dishonest employers or insurers. • The Administration is open to views as to whether Clause 38 should be retained	• Data access and correction are crucial rights for the protection of an individual's personal data. Clause 38 in effect nullifies section 17A of the PDPO which provides for an HCR to authorize a person in writing to make a DAR or DCR. It therefore reduces the HCR's autonomy in handling his personal data. This is particularly problematic where the HCR falls sick and requires assistance from others in pursuing the requests.

	or not.	• While Clause 38 of the Bill applies to the HCRs' health data under the eHRSS only, the HCRs are still entitled under the PDPO to exercise the rights of data access and correction through their authorized persons in relation to their health data maintained separately with the HCPs. The inconsistent treatment of health data under the Bill and the PDPO will be confusing. • The Administration has not provided statistics to support that authorisation is subject to abuse by dishonest employers or insurers. • The PCPD objects to the proposal.
Part 5 and Clause 41	**Offence - Unauthorized access by non-computer means** • To criminalize the act of *"unauthorized access"* not followed by any malicious act could be disproportionate as unauthorized access to personal data under the PDPO is not an offence.	• The PDPO governs all personal data regardless of data sensitivity. During the public consultation for the review of the PDPO in 2010, there was general support for the proposal to introduce tighter control over sensitive personal data. The proposal was not taken forward by the Administration as it failed to identify a consensus on the coverage of sensitive personal data. However, there should be little argument that health data is sensitive and should therefore, according to the majority views expressed in the

		2010 public consultation, be afforded a higher level of protection. • Unauthorized access to personal data without subsequent malicious act may not be as innocent as it seems to be. For instance, a person who accesses eHR data without authorisation and collects the personal data may not have an immediate plan in mind as regards how to take advantage of the data. He may simply "reserve" it for some undefined future use. There was a case concerning the conviction of a staff of the Inland Revenue Department for misconduct in public office in copying the personal data of tax payers without the authority of the Commissioner of Inland Revenue. The convicted staff had never used any of the copied data but claimed that the data might be of use to him in future. • If the Administration thinks that criminal sanction is too harsh, it may wish to consider other penalties. For example, section 59(1) of the PCEHR Act imposes a civil penalty on a person who *collects* from the PCEHR system health information without authorisation and that person knows or *is reckless* as to that fact.

	Offence - Creating an offence against misuse of eHR data • Difficult to define "*misuse*" as it could cover a wide range of scenarios • Not appropriate to create an offence to cover generally all *"misuses of eHR data"* • "*Misuse*" of personal data under DPP3 of PDPO is not an offence	• The PCPD repeats his comments above that patients' health data is sensitive and should be afforded greater protection than that provided under the PDPO. No offence is proposed under the Bill for misuse of the eHR for purposes unrelated to the healthcare of the HCRs except that it is an offence under clause 46 of the Bill to use the eHR data for direct marketing purpose. This is an omission which needs to be addressed. • Section 64 of the PDPO[4] provides that it is an offence to disclose personal data obtained without the data user's consent but certain conditions must be fulfilled. The applicability of this section is further limited in small HCPs such as a one-doctor clinic where the wrongdoer is the data user and therefore the issue of consent will not arise. • Any use which is different from that permitted under the Bill will be *"misuse"*. The PCPD disagrees with the Administration's view that an offence on *"misuse"* of eHR in general should not be imposed just because there are different extent and scenarios of

[4] 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 unauthorized 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.

		"misuse". There are examples in existing ordinances for criminalising a general misuse of personal data for purposes other than that for which the data is collected. For example, use of voters' personal data contained in an election register for purposes other than election is an offence[5].
Clause 57(2)	**Limitation of Liability:** **Inspection of local Electronic Medical Record (eMR) systems of HCPs** • The Administration considers that it is not reasonably practicable for the eHRC to inspect or commit to inspect local eMR systems of HCPs to ascertain (1) whether the Electronic Health Record Sharing System Ordinance (the Ordinance) is complied with; and (2) whether any sharable data provided to the eHRSS is accurate. The reasons are:	• The PCPD objects to this proposed limitation which in effect belittles and discredits the eHRC's statutory functions to regulate and supervise the sharing and use of eHR (clause 48(1)(b)) among the HCPs and to supervise their compliance with the Ordinance (clause 48(1)(c)). It calls in question how the eHRC could exercise his supervisory and oversight role effectively. For example, the eHRC has to make decisions to suspend or cancel registration of HCPs. Relieved of any obligation to conduct inspection of the HCPs' local eMR systems, it is conceivable that such decisions will only be made as a response to crises such as serious data

[5] See section 22(3) of the Electoral Affairs Commission (Registration of Electors) (Legislative Council Geographical Constituencies) (District Council Constituencies) Regulation (Cap.541A) and section 42(3) of the Electoral Affairs Commission (Registration) (Electors for Legislative Council Functional Constituencies) (Voters for Election Committee Subsectors) (Members of Election Committee) Regulation (Cap.541B)

	➢ Local eMR systems are systems used by individual HCP. They are not part of the eHRSS and thus fall outside the ambit of the eHRC. ➢ Local eMR systems may contain sensitive information not relevant to eHR sharing; inspection will be highly intrusive and deter HCPs from joining the eHRSS. ➢ The eHRC has no expertise and historical knowledge to check the content accuracy of the data in the local eMR systems, as they are largely professional assessment of healthcare professionals. • The HCPs are subject to the regulation of the PCPD under the PDPO. It is the obligation of the HCPs as data users to ensure security of their local eMR systems and the accuracy of the data. • The Administration benchmarks the eHRSS with the inter-bank clearing system which accepts transactions from	breaches on the part of the HCPs, when ideally it should be made as a preventative measure before things get out of control. • The PCPD notes that the Administration is obsessive about the integrity of the eHR in the eHRSS when considering the safe deposit box. This is in sharp contrast to exonerating the eHRC from inspecting the local eMR systems and ensuring the security and content accuracy of the data it uploads to the eHRSS. • Indeed such assurance is the obligation of eHRC as a data user under DPP4 and DPP2(1) respectively of the PDPO. However, with the proposed limitation, any direction from the PCPD for the eHRC to conduct inspection of the local eMR systems is impossible. This effectively reduces the PCPD's enforcement power that may be invoked against the eHRC to ensure the latter's compliance with the PDPO. • The Administration's worry over unmeritorious litigations may have been overstated, taking into account that the standard of compliance with DPP2(1) and DPP(4) is simply to *take all reasonably practicable steps*. • The PCPD further notes the Administration's comments that the eHRC may not be professionally equipped to conduct the inspection and inspecting information not relevant to eHR is highly intrusive. These are logistical problems which can be resolved. For example, the inspection could be designed to focus

	various banks but does not inspect the banks' local systems. • Similar clauses that protect the Administration from unmeritorious litigations are found in a number of ordinances concerning land, buildings and infrastructure.	on the relevant data of local eMR systems. In any event, the eHRC should be meeting his obligations if he takes all reasonably practicable steps in good faith. • It is not entirely appropriate to compare the eHRSS with the inter-bank clearing system. A closer analogy is the Hospital Authority which manages public hospitals in Hong Kong. It sets up policies and guidelines for adoption by public hospitals in the protection of patients' personal data, and ensures compliance through inspections and other audit work. Another relevant benchmark is TransUnion, a credit reference agency that collects consumers' 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[6]. The credit reference agency is not exonerated of its obligations as a data user under DPP2(1) in any way. • Lastly, under the PCEHR Act 2012, the system operator of

[6] 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

		PCEHR in Australia, which performs similar functions as the eHRC, is not offered any exclusion from inspection[7]. • All examples given by the Administration for limiting liability are not exemptions from the liability or responsibility for personal data protection. • The PCPD will not shirk his responsibility to monitor compliance with the PDPO by individual HCPs. But inevitably, in the interest of fairness in deploying his limited resources among all data users in Hong Kong, he is unable to focus on HCPs. The eHRC no doubt is much better positioned and resourced to exercise oversight over the HCPs. Abdication of this responsibility on the part of the eHRC is counter-productive to promote compliance with the PDPO and the Ordinance by the HCPs.

[7] 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).