

**立法會**  
**Legislative Council**

LC Paper No. CB (2)1965/14-15  
(These minutes have been  
seen by the Administration)

Ref : CB2/BC/6/13

**Bills Committee on Electronic Health Record Sharing System Bill**

**Minutes of the eighth meeting**  
**held on Tuesday, 11 November 2014, from 4:30 pm to 7:30 pm**  
**in Conference Room 3 of the Legislative Council Complex**

**Members present** : Hon Charles Peter MOK, JP (Chairman)  
Hon Emily LAU Wai-hing, JP  
Prof Hon Joseph LEE Kok-long, SBS, JP, PhD, RN  
Hon Cyd HO Sau-lan, JP  
Dr Hon LEUNG Ka-lau  
Hon Alan LEONG Kah-kit, SC  
Hon Alice MAK Mei-kuen, JP  
Dr Hon KWOK Ka-ki  
Dr Hon Fernando CHEUNG Chiu-hung  
Dr Hon Helena WONG Pik-wan  
Dr Hon Elizabeth QUAT, JP  
Ir Dr Hon LO Wai-kwok, BBS, MH, JP

**Members absent** : Hon CHEUNG Kwok-che  
Hon WU Chi-wai, MH  
Hon CHAN Han-pan, JP

**Public Officers attending** : Item I  
Mr Sidney CHAN, JP  
Head (eHealth Record)  
eHealth Record Office  
Food and Health Bureau

Ms Ida LEE  
Deputy Head (eHealth Record)  
eHealth Record Office  
Food and Health Bureau

Dr Antonio SEK  
Chief Manager (eHealth Record)  
eHealth Record Office  
Food and Health Bureau

Mrs Juliet CHENG  
Chief Systems Manager (eHealth Record)  
eHealth Record Office  
Food and Health Bureau

Dr W N WONG  
Senior Health Informatician (eHealth Record) Special Duties  
eHealth Record Office  
Food and Health Bureau

Ms Rayne CHAI  
Acting Senior Assistant Law Draftsman  
Department of Justice

Mr Patrick YEUNG  
Senior Government Counsel  
Department of Justice

Ms Carmen CHAN  
Acting Senior Government Counsel  
Department of Justice

**Attendance by invitation** : Office of the Privacy Commissioner for Personal Data

Mr Allan CHIANG  
Privacy Commissioner for Personal Data

Ms Sandra LIU  
Senior Legal Counsel

**Clerk in attendance** : Ms Maisie LAM  
Chief Council Secretary (2) 5

**Staff in attendance** : Miss Carrie WONG  
Assistant Legal Adviser 4

Ms Janet SHUM  
Senior Council Secretary (2) 5

Ms Michelle LEE  
Legislative Assistant (2) 5

---

Action

**I. Meeting with the Office of the Privacy Commissioner for Personal Data and the Administration**

[File Ref.: FH CR 1/1/3781/10, LC Paper Nos. CB(2)1515/13-14(01), CB(2)1551/13-14(01), CB(2)1580/13-14(03), CB(2)1775/13-14(02), CB(2)1873/13-14(01), CB(2)2045/13-14(01) to (03), CB(2)2078/13-14(01), CB(2)2308/13-14(01) to (02), CB(2)2317/13-14(01), CB(2)221/14-15(01) to (02) and CB(3)575/13-14]

The Bills Committee deliberated (index of proceedings attached at **Annex**).

Admin

2. The Bills Committee requested the Administration to provide a written response on the following -

- (a) to re-affirm the latest direction of the study on provision of additional means for healthcare recipients to restrict access to their sharable data under the Electronic Health Record Sharing System ("eHRSS") which was targeted to commence in the first year of Stage Two of the Electronic Health Record Programme;
- (b) to clarify whether clause 12(6)(a)(i) and (b)(i) as presently drafted would render it not viable for registered healthcare recipients ("HCR") to request prescribed healthcare providers and referral healthcare providers, to which they had given a sharing consent, not to provide to eHRSS certain parts of their health data within the sharable scope; and
- (c) to provide a comparison table on the new offences proposed under the Bill and relevant offences as currently provided for under existing laws and setting out whether there was any overlapping in the scope of coverage of the offences.

Action

3. The Administration undertook to consider whether it was practical and proportionate to criminalize any use of data and information contained in the electronic health record ("eHR") of an HCR which fell outside the scope of use of eHR specified under clauses 26, 27, 28 and 29.

4. The Chairman suggested and members agreed that the above issue could be further deliberated during the clause-by-clause examination of the Bill.

**II. Any other business**

5. There being no other business, the meeting ended at 7:22 pm.

Council Business Division 2  
Legislative Council Secretariat  
24 July 2015

**Proceedings of the eighth meeting of  
the Bills Committee on Electronic Health Record Sharing System Bill  
held on Tuesday, 11 November 2014, from 4:30 pm to 7:30 pm  
in Conference Room 3 of the Legislative Council Complex**

Time marker	Speaker	Subject(s)/Discussion	Action required
<i>Agenda item I: Meeting with the Office of the Privacy Commissioner for Personal Data and the Administration</i>			
000130 - 000317	Chairman	Opening remarks	
000318 - 000436	Chairman Admin	<p><u>Additional access control by registered healthcare recipients over data sharing</u></p> <p>Powerpoint presentation by the Administration on its response to issues of concerns raised by the Privacy Commissioner for Personal Data ("PCPD") on the provision of additional access control by registered healthcare recipients ("HCRs") (viz. a "safe deposit box" feature) over their health data contained in the Electronic Health Record Sharing System ("eHRSS").</p> <p>[Item 4 in LC Paper No. CB(2)2148/13-14(01)]</p>	
000437 - 001216	Chairman PCPD	<p>PCPD highlighted his response to the draft Committee Stage amendments ("CSAs") proposed by the Administration concerning the addition of a new clause 35A, details of which were set out in his letter dated 22 September 2014 (LC Paper No. CB(2)2317/13-14(01)).</p> <p>On the provision of additional access control in eHRSS, PCPD's remarks that it would be difficult for a full consensus be reached by different quarters of the community over the issue. That said, registered HCRs should be provided with additional access control over their health data, in order to uphold their right not to disclose certain health data to the prescribed healthcare providers ("HCPs") and protect them from discrimination which otherwise could result from inadequate access control of particularly sensitive health data. Hence, there was a need to provide expressly in the Bill that a "safe deposit box" feature would be provided in eHRSS within a timeframe to be specified.</p>	
001217 - 002452	Chairman Dr KWOK Ka-ki Dr Elizabeth QUAT Ms Emily LAU Admin	<p>Dr KWOK Ka-ki and Dr Elizabeth QUAT's concurrence with PCPD's views that registered HCRs should be provided with additional access control over the sharing of their health data in eHRSS, and there was a need to provide expressly in the Bill that a "safe deposit box" feature would be provided in eHRSS within a specified timeframe for the following reasons -</p> <p>(a) the Administration should take heed of patient groups' call for the provision of a "safe deposit box" feature in eHRSS so that patients could gain confidence in its privacy safeguards and become more willing to join</p>	

Time marker	Speaker	Subject(s)/Discussion	Action required
		<p>eHRSS upon its commencement of operation. It was noted that during the public consultation conducted in 2011, 18 among the 23 responses received on the issue were against the proposal of not providing "safe deposit box" in eHRSS, whereas the remaining five responses indicated support or no objection to the proposal that there should not be any "safe deposit box" in eHRSS;</p> <p>(b) there was no reason that the withholding of certain health data from the electronic health record ("eHR") of the registered HCRs would affect the quality of healthcare provided by the prescribed HCPs, as it was incumbent upon the HCPs to exercise their own professional judgement when using eHR as a clinical reference. Where necessary, they could get the medical information required to make an accurate diagnosis and/or treatment directly from the HCRs concerned during consultation. In fact, the eHR kept in eHRSS could not be construed as a complete set of health record of the registered HCRs, as not all health data contained in the medical records kept by individual HCPs fell within the sharable scope of eHRSS; and</p> <p>(c) the Administration's argument that the proposal to introduce a "safe deposit box" feature in eHRSS should not be taken forward at this stage as none of the overseas experiences in this regard was particularly successful to date was not sound. In Dr Elizabeth QUAT's view, a working group comprising experts from the information technology ("IT") sector could be set up to provide technical advice to the Administration to take forward the matter.</p> <p>While agreeing with PCPD's view that extra access control should be provided in eHRSS, Ms Emily LAU sought further explanation from the Administration on the difficulties for it to introduce the feature at this stage.</p>	
002453 - 003038	Chairman Admin	<p>The Administration's response that -</p> <p>(a) provision of a feature in the eHRSS to enable registered HCRs to restrict disclosure of certain health data was not included as an item in the eHRSS developed during Stage One (from 2009-2010 to 2013-2014) of the ten-year Electronic Health Record Sharing Programme ("eHR Programme). Noting that there were diverse views over the issue during the public consultation conducted in 2011 and at the meeting of the Bills Committee on 26 May 2014 to receive views from deputations on the Bill, the Administration had already undertaken to commence a study on additional access control for sensitive data, with reference to overseas experiences, in the first year of the Stage Two eHR Programme; and</p> <p>(b) in view of PCPD and members' concerns over the issue, the Administration would ensure that the study would be</p>	

Time marker	Speaker	Subject(s)/Discussion	Action required
		<p>conducted along a positive direction, with a view to developing and implementing some form of new device or arrangement enabling additional choice for HCRs over the disclosure of their data. The Administration would consult the relevant stakeholders (including patient groups and healthcare-related professional bodies), as well as the Panel on Health Services of the Legislative Council on the way forward upon completion of the study. The implementation timetable would, however, depend on the complexity of the work involved.</p>	
003039 - 004402	<p>Chairman Dr KWOK Ka-ki Dr Elizabeth QUAT</p>	<p>Dr KWOK Ka-ki welcomed the Administration's undertaking that the study would be conducted along a positive direction, and urged the Administration to ease the concerns raised by healthcare professionals as far as practicable in the study, with a view to gaining their support for the provision of a feature in eHRSS to enable HCRs to restrict disclosure of certain health data during the next round of consultation.</p> <p>Given that it would be difficult for a full consensus be reached by different stakeholders over the issue, Dr KWOK Ka-ki and Dr Elizabeth QUAT maintained the view that there was a need to provide expressly in the Bill that the "safe deposit box" feature would be provided in eHRSS.</p> <p>The Administration's response that -</p> <p>(a) "safe deposit box" was used to describe a broad general concept with no commonly accepted definition or a standard technical design. Those countries with their respective eHR sharing arrangements in place, such as Australia, France and the United Kingdom, were allowing different extents of control to access to records by different means. It was neither desirable, nor appropriate, to stipulate the provision of a particular form of a "safe deposit box" in the Bill. The Bill as currently drafted, which was technology neutral to cater for future advancement in health IT, did not preclude the provision of such feature in the future; and</p> <p>(b) the Administration would gauge the view of the Steering Committee on Electronic Health Record Sharing ("eHRSC"), which comprised representatives of key stakeholders in different sectors, in the course of working out a feasible and acceptable option to enable additional choice for HCRs over the disclosure of their health data in eHRSS. It would also relay to eHRSC the strong view of members of the Bills Committee on the need to provide such choice for HCRs.</p>	
004403 - 005419	<p>Chairman PCPD Dr LEUNG Ka-lau Ms Emily LAU Dr Elizabeth QUAT</p>	<p>PCPD's strong view that there should be express provisions in the Bill to provide for the registered HCRs to exercise some form of control over the scope of data sharing in eHRSS. To do so would not pre-empt the future design of the relevant feature in eHRSS as there was no need to specify in detail the</p>	

Time marker	Speaker	Subject(s)/Discussion	Action required
		<p>form of control in the Bill.</p> <p>Dr Elizabeth QUAT's expression of concurrence that the spirit that registered HCRs could exercise some form of control over the scope of data sharing in eHRSS, together with an implementation timeframe, should be stipulated in the Bill.</p> <p>Ms Emily LAU's remarks that the drafting of any amendments to the Bill to enable additional choice for HCRs over the disclosure of their health data in eHRSS should be clear in order to avoid future dispute.</p> <p>Dr LEUNG Ka-lau's enquiry as to whether clause 12(6)(a)(i) and (b)(i), which provided that a registered HCR or a substitute decision maker ("SDM") of an HCR might give a sharing consent to a prescribed HCP, should be amended to the effect that a registered HCR (or his/her SDM) could request a prescribed HCP not to provide to eHRSS certain parts of his/her health data that fell within the sharable scope.</p>	
005420 - 005857	Chairman Admin	<p>The Administration's response that -</p> <p>(a) it aimed to complete the study on additional access control for data sharing as early as practicable during Stage Two of the eHR Programme. It could re-assure members in writing that the study would be conducted along a positive direction, with a view to developing and implementing some form of new device or arrangement enabling additional choice for HCRs over the disclosure of their data in eHRSS; and</p> <p>(b) it was, however, difficult to stipulate the concept of an IT feature in the Bill when the design of which had yet been commenced. As regards Dr LEUNG Ka-lau's proposal to allow registered HCRs to have full control of the types of sharable data that could be uploaded to eHRSS under clause 12(6), it would pre-empt the future design of the new device or arrangement which could otherwise, for instance, not allow an HCR to withhold certain essential health data (such as allergies and medication) or enable the prescribed HCPs to make their professional judgement as to whether an HCR's request to withhold a particular sharable data should be acceded to.</p>	<b>Admin</b>
005858 - 011614	Chairman Dr LEUNG Ka-lau Admin	<p>Making reference to the current arrangement of the Hospital Authority ("HA") that clinical records relating to the mental health of its patients would not be uploaded to its Clinical Management System for sharing within HA in view of their sensitive nature, Dr LEUNG Ka-lau maintained the view that -</p> <p>(a) clause 12(6) as currently drafted would result in an HCR not being able to hold an HCP liable for the uploading of any of his/her sharable data to eHRSS even though he/she had requested the HCP not to do so, as a sharing</p>	



Time marker	Speaker	Subject(s)/Discussion	Action required
		<p>consent had already been given to the HCP; and</p> <p>(b) there was a need to amend clause 12(6) to allow HCRs to request HCPs not to provide certain parts of their sharable data to eHRSS, regardless of whether or not a "safe deposit box" feature would be provided in eHRSS in the future.</p> <p>The Administration's response that -</p> <p>(a) the respective requirements stipulated in the codes of practices issued under the Hospitals, Nursing Homes and Maternity Homes Registration Ordinance (Cap. 165) and the Medical Clinics Ordinance (Cap. 343), as well as the codes of conduct of various healthcare professionals was that these entities or persons had to maintain accurate medical records of their patients, be they handwritten, printed or in electronic form; and</p> <p>(b) under the design or workflows of the eHRSS developed under the Stage One eHR Programme, all health data of the registered HCRs falling within the sharable scope would be uploaded to eHRSS with no exclusion once the prescribed HCP had entered such data into its local electronic medical/patient record ("eMR/ePR") systems, if its eMR/ePR system had the capability to interconnect with eHRSS.</p> <p>At the request of Dr LEUNG Ka-lau, the Administration undertook to clarify in writing whether clause 12(6)(a)(i) and (b)(i) as currently drafted would render it not viable for registered HCRs to request prescribed HCPs and referral healthcare providers, to which they had given a sharing consent, not to provide to eHRSS certain parts of their health data within the sharable scope.</p>	<b>Admin</b>
011615 - 012736	Chairman Ms Cyd HO Dr Helena WONG	<p>Ms Cyd HO's view that registered HCRs should be provided with some form of control over the disclosure of their data in eHRSS, say, through introducing a "safe deposit box" feature in eHRSS or CSAs to clause 12(6) as proposed by Dr LEUNG Ka-lau. In the case of the former, it would obviate the need for HCPs to keep separate records of the data the HCRs requested to withhold from sharing in eHRSS. To take forward the matter, the Bills Committee could consider proposing relevant CSAs to this effect and PCPD might submit his proposal in this regard for the Bills Committee's consideration.</p> <p>Dr Helena WONG's enquiry as to whether the Administration would take on board the Bills Committee's view to provide expressly in the Bill that registered HCRs would be provided with some form of control over data disclosure in eHRSS.</p> <p>The Administration's reiteration of its position that the Bill was technology neutral to cater for future advancement in IT.</p>	

Time marker	Speaker	Subject(s)/Discussion	Action required
		It was neither desirable, nor appropriate, to stipulate the provision of a particular form of "safe deposit box" in the Bill.	
012737-013303	Chairman PCPD Dr Elizabeth QUAT	<p>PCPD did not subscribe to the Administration's explanations and maintained the view that the spirit that registered HCRs could exercise some form of control over the scope of data sharing in eHRSS should be spelt out the Bill. He would be more than happy to suggest amendments to the Bill in this regard for the consideration of the Bills Committee.</p> <p>Dr Elizabeth QUAT shared PCPD's view and said that she would propose CSAs to the Bill if the Administration did not take heed of members' and PCPD's views on this issue, as the decision of patients to join eHRSS would hinge on their confidence in its privacy safeguards.</p>	
013304 - 013902	Chairman Admin PCPD	<p><u>Offences</u></p> <p>Powerpoint presentation by the Administration on its response to issues of concerns raised by PCPD on unauthorized access to eHRSS by non-computer means and misuse of eHR in general.</p> <p>[Item 5 in LC Paper No. CB(2)2148/13-14(01)]</p>	
013903 - 015633	Chairman PCPD	<p>PCPD's view that -</p> <ul style="list-style-type: none"> <li>(a) unauthorized access to data or information contained in an eHR other than the use of a computer should also be an offence. During the public consultation for the review of the Personal Data (Privacy) Ordinance (Cap. 486) ("the Privacy Ordinance") in 2009, a more stringent regulatory regime for sensitive personal data (including health data) was proposed but the proposal was not taken forward by the Administration. One of the reasons was that there were no mainstream views in the community on the scope of sensitive personal data. There should, however, be little argument that health data was sensitive in nature;</li> <li>(b) misuse of data or information contained in an eHR for purposes unrelated to the healthcare of an HCR (in addition to the use of eHR data for direct marketing purpose as provided under clause 46) should be made an offence given the sensitive nature of health data; and</li> <li>(c) if criminal sanction for unauthorized access by non-computer means and misuse of eHR data was considered too harsh, consideration could be given to imposing other types of penalty, such as civil penalty as in Australia.</li> </ul> <p>The Administration's advice that -</p> <ul style="list-style-type: none"> <li>(a) in light of the diverse views received during the public consultation for the review of the Privacy Ordinance on the coverage of sensitive personal data, the mode of regulation and sanctions, the Administration decided not</li> </ul>	

Time marker	Speaker	Subject(s)/Discussion	Action required
		<p>to institute a specific regulatory regime for sensitive personal data at that time; and</p> <p>(b) the new offences introduced under the Bill did not cover all health records but were specific to the operation of eHR sharing. Hence, it might be more appropriate to address the need to accord better protection to health records, if considered necessary, under the privacy protection regime in the Privacy Ordinance. It should be noted that relevant provisions of the Privacy Ordinance would be applied to data and information contained in eHR that fell within the meaning of "personal data" under the Privacy Ordinance unless otherwise specified.</p> <p>Dr LEUNG Ka-lau's enquiry about what would constitute access to data or information contained in an eHR. In particular, whether a doctor who had overheard, or participated in, the discussion among doctors on a case of an HCR making reference to the data or information contained in his/her eHR would be regarded as having collected and used the data or information contained in the eHR.</p> <p>PCPD's advice that under the Privacy Ordinance, data meant any representation of information (including an expression of opinion) in any document, and included a personal identifier. Use of personal data included disclosing or transferring the data. In the scenario cited by Dr LEUNG Ka-lau, the doctor had collected and used personal data if he had recorded the information in writing and disclosed or transferred it.</p>	
015634 - 020517	Chairman Admin Dr LEUNG Ka-lau	<p>Dr LEUNG Ka-lau's enquiry about whether there was any overlapping in the scope of coverage of the new offences relating to accessing, damaging or modifying data or information as proposed under clause 41 and the existing offence of "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance (Cap. 200).</p> <p>Pointing out that the original policy intent of section 161 of the Crimes Ordinance was to criminalize access to a computer for acts preparatory but falling short of the commission of a fraud, the Chairman was concerned about an upsurge in the number of prosecutions cases pertaining to section 161 of the Crimes Ordinance in recent years. In his view, provisions of the Bill, if enacted, should be invoked for illegal acts that were specific to the data or information contained in the eHR.</p> <p>The Administration's advice that the act to be criminalized under clauses 41(6), (7) and (8) was broader to cover not only "access", but also "modification" and "impairment to the accessibility, reliability, security or processing", whereas the offence was specifically directed at "data or information in an eHR" as opposed to "computer" generally. Any persons who committed these offences would be subject to a maximum penalty of five-year-imprisonment on conviction upon indictment, which was the same as the penalty for contravening section 161 of the Crimes Ordinance. In determining which</p>	

Time marker	Speaker	Subject(s)/Discussion	Action required
		<p>legal provision should be invoked when laying charges, the law enforcement agent would give due regard to the circumstances of each individual case, and in general, the more specific provision would be invoked.</p> <p>Dr LEUNG Ka-lau's request for the Administration to provide a comparison table on the new offences proposed under the Bill and relevant offences as currently provided for under the existing laws and setting out whether there was any overlapping in the scope of coverage of the offences.</p>	<b>Admin</b>
020518 - 021440	<p>Chairman Dr Elizabeth QUAT PCPD Admin</p>	<p>In response to Dr Elizabeth QUAT, the Administration's clarification that -</p> <p>(a) an act to knowingly cause a computer to perform a function so as to obtain unauthorized access to data or information contained in an eHR (such as hacking), and an access to data or information contained in an eHR with criminal or dishonest intent (such as with a view to dishonest gain for the person or for another or with a dishonest intent to cause loss to another) were different offences under clause 41(1) and (6) respectively; and</p> <p>(b) criminalizing a particular act was a serious matter which had to be justified with compelling reasons. To criminalize the mere act of unauthorized access to personal data not followed by any malicious act could arguably be disproportionate. If it was considered that such an act should be criminalized in general, amending the Privacy Ordinance would be more appropriate in the light of the across-the-board implications. Once the Privacy Ordinance was amended to such effect, a review of the arrangement for data or information contained in eHR would be conducted accordingly.</p> <p>Dr Elizabeth QUAT's enquiry about whether an unauthorized access to data or information contained in an eHR by non-computer means (such as reading eHR from the screen due to the act of somebody forgetting to log out), with or without disclosing the data or information so collected afterwards (such as posting the data or information on an online social networking platform), would be an offence under the Privacy Ordinance; and PCPD's advice that -</p> <p>(a) the mere act of accessing one's personal data without consent was not an offence under the Privacy Ordinance. A person committed an offence under section 64 of the Privacy Ordinance if the person disclosed any personal data of a data subject which was obtained from a data user without the data user's consent, with an intent to obtain gain in money or other property, whether for the benefit of the person or another person, or to cause loss in money or other property to the data subject; and</p> <p>(b) it should, however, be noted that data protection principle 3 ("DDP3") provided that personal data should</p>	

Time marker	Speaker	Subject(s)/Discussion	Action required
		<p>not, without the prescribed consent of the data subject, be used for a new purpose. A data user's disclosure of the data and information contained in an eHR on an online social networking platform, which was not within the original purpose of collection and in the absence of prescribed consent from the data subjects, might contravene DDP3. An enforcement notice would be served on the data user concerned to direct the data user to remedy the contravention. Non-compliance of the enforcement notice was an offence.</p>	
021441 - 022706	Chairman Dr Elizabeth QUAT PCPD Admin	<p>Dr Elizabeth QUAT's expression of disagreement with the Administration's view that it was inappropriate to take forward the suggestion to criminalize unauthorized access to data or information in eHR without subsequent malicious act as eHR, which only contained health data within the defined sharable scope, formed only part of the health records of an HCR; and her view that the unique arrangement of data sharing under eHRSS had made it necessary for additional safeguards be provided in order to instil confidence of HCRs in eHRSS.</p> <p>The Chairman's view of the need to strike a proper balance between the interests of the data subjects and data users in determining how far the data and information contained in eHR should be protected. In response to Dr Elizabeth QUAT's enquiry as to how the data and information contained in eHR could be better protected, PCPD's advice that -</p> <ul style="list-style-type: none"> <li>(a) unauthorized access to personal data without subsequent malicious act might not be as innocent as it seemed as the person might intend to keep the data concerned for future use. There was a case whereby a staff of the Inland Revenue Department was convicted for copying the personal data of tax payers without the authority of the Commissioner of Inland Revenue. The staff had never used any of the copied data but claimed that the data might be of use to him in future; and</li> <li>(b) to criminalize across-the-board unauthorized access to personal data without subsequent malicious act required introducing amendments to the Privacy Ordinance. The lack of timetable of the Administration for conducting another round of comprehensive review of the Privacy Ordinance had made it impossible for him to take the proposal forward at this stage. Introducing CSAs to the Bill to such effect could at the very least accord better protection to data and information in the eHR which was sensitive in nature. Some form of pecuniary fines, instead of criminal sanction, could be imposed on such access.</li> </ul> <p>The Administration's reiteration of the protection provided under clause 41(1) and (6), the views received during public consultation for the review of the Privacy Ordinance in 2009, and its position that it would be more appropriate to defer to</p>	

Time marker	Speaker	Subject(s)/Discussion	Action required
		PCPD to separately raise the issue again for consultation with the public and the Administration.	
022707 - 022906	Chairman Admin	On the Chairman's enquiry about the standard adopted for proving a criminal or dishonest intent under clause 41(6), the Administration's advice that what constituted a criminal or dishonest intent would be a matter of fact for the court to decide in each individual case.	
022907 - 023457	Dr Elizabeth QUAT Chairman PCPD Admin	<p>Dr Elizabeth QUAT's reiteration of her view that it was not desirable not to penalize the wrongdoing of unauthorized access to data or information contained in an eHR by non-computer means not followed by any malicious act, as the access would intrude into personal data privacy.</p> <p>In response to Dr Elizabeth QUAT's enquiry about whether PCPD had any proposed amendments to provisions of the Bill to enhance protection in this regard, PCPD's reiteration that some form of pecuniary fines could be imposed to provide a deterrent against such access as in the case of acts related to minor traffic offences.</p> <p>The Chairman's remarks that the issue could be further deliberated during the clause-by-clause examination of the Bill.</p>	
023458 - 024212	Chairman PCPD Dr Elizabeth QUAT Admin	<p>Dr Elizabeth QUAT's enquiry as to whether consideration could be given to including cyber-bullying acts using another person's data or information contained in an eHR as an offence under the Bill.</p> <p>While considering that any offence on misuse of the data or information contained in eHR should be against specific acts as there were different extents and various scenarios of misuse of such data and information and no list could be exhaustive, the Chairman's remarks that there was currently no law in Hong Kong defining or governing cyber-bullying.</p> <p>PCPD's view that in addition to making the use of data or information contained in eHR for direct marketing purpose an offence under clause 46, any other uses for purposes other than that for which the data and information was collected should be made an offence. As a reference, using voters' personal data contained in the voter register for purposes other than election was an offence.</p> <p>Dr Elizabeth QUAT's expression of concurrence with PCPD's view; and the Administration's response that -</p> <p>(a) clauses 26 to 29 provided that the data and information contained in eHR might be used for improvement of healthcare provided (or to be provided) to the registered HCR, research and statistics related to public health or public safety, the prevention or control of diseases and the enhancement of disease surveillance or investigation, and other uses permitted by, or under, any other law; and</p>	

Time marker	Speaker	Subject(s)/Discussion	Action required
		(b) from the law enforcement or prosecution perspective, it might not be appropriate to create an offence to cover generally all misuses of data and information in eHR. It would consider whether it was practical and proportionate to criminalize any use of data and information contained in the eHR of a registered HCR which fell outside the scope of use of eHR specified under clauses 26 to 29. Meanwhile, the example of the personal data contained in voter register raised by PCPD was under very different context. It was not appropriate to draw direct reference from it.. At present, voter register was accessible to the public for inspection, whereas the use of data and information in an eHR of a registered HCR would be limited by the Bill as well as protected by system design, and stringent security and privacy measures, with limited access.	<b>Admin</b>
024213 - 025018	Chairman Admin PCPD Dr Elizabeth QUAT	<p><u>Limitation of public liability</u></p> <p>PCPD's view that clause 57(2) should be deleted, as it called in question how the Commissioner for the Electronic Health Record ("eHRC") could exercise the supervisory and oversight role effectively if he/she was not obliged to inspect, or commit to inspect, an electronic medical record ("eMR") system of the HCPs. The provision would also reduce his enforcement power that might be invoked against eHRC, who was regarded as a data user in the context of the Privacy Ordinance, to ensure the use of eHRSS would comply with the requirements under the Privacy Ordinance.</p> <p>The Administration's advice that having considered PCPD's concern in this regard, it would move CSAs to delete clause 57(2); and Dr Elizabeth QUAT's expression of support for the Administration's latest position.</p>	
<i>Agenda item II: Any other business</i>			
025019 - 025046	Chairman	Closing remarks	