Bills Committee on Electronic Health Record Sharing System Bill

Summary of issues involving major proposed amendments to the Bill raised by members and/or the Privacy Commissioner for Personal Data and the Administration's position

Views from members and/or the Privacy Commissioner for Personal Data	The Administration's latest position	Draft Committee Stage amendments to the Bill
Clause 16 - Sharing consent taken to be given		
Pursuant to clause 16(1) and (2), a healthcare recipient ("HCR") or a substitute decision maker ("SDM") of an HCR was taken to have given a sharing consent to the Hospital Authority ("HA") and the Department of Health ("DH") when the HCR or SDM concerned gave a joining consent. Some members were of the view that the above provision should be amended to the effect that an HCR or his/her SDM was allowed to opt out from this arrangement.	HA and DH, being healthcare providers ("HCPs") in the public sector serving the largest number of patients, held a vast amount of health data which would be the essential building blocks of the life-long electronic health record ("eHR") of registered HCRs. While the opt-out arrangement (the implementation of which would require modifying the design of the Electronic Health Record Sharing System ("the System") which would take no less than 12 months to complete) was not technically infeasible, it was highly undesirable from policy perspective as it was not conducive to the realization of the objective of the System to foster public-private collaboration in healthcare delivery.[1]	Nil

[1] Please refer to item (b) of LC Paper No. CB(2)2308/13-14(02) for details of the Administration's response.

Views from members and/or the Privacy Commissioner for Personal Data	The Administration's latest position	Draft Committee Stage amendments to the Bill
Proposed new Division 3A: Sharing restriction		
(a) The Privacy Commissioner for Personal Data ("the Privacy Commissioner") and some members were of the strong view that registered HCRs should be provided with additional access control over their health data contained in their eHR (viz. the provision of a "safe deposit box" feature for separate storage of certain health data), in order to uphold their right not to disclose certain health data to the prescribed HCPs and protect them from discrimination which otherwise could result from inadequate access control of particularly sensitive health data. Specifically, the Privacy Commissioner suggested (i) adding a new subclause to clause 12 to allow a registered HCR to exercise control over the consent given by him/her to share his/her data; and (ii) adding a definition for "sharing control" under clause 2 to allow the Secretary for Food and Health to determine or specify the appropriate form of control by way of gazette.[2]	(a) The full development plan of the System was a 10-year programme which straddled from 2009-2010 to 2018-2019 and comprising two stages. The "safe deposit box" feature was not included as an item in the scope of Stage One of the Electronic Health Record Programme (from 2009-2010 to 2013-2014). The Administration would conduct, in the first year of Stage Two of the Programme, a study on enhancing HCRs' choice along a positive direction, with a view to developing and implementing some form of new device or arrangement enabling additional choice for registered HCRs over the disclosure of their data. The Administration would introduce Committee Stage amendments ("CSAs") to the Bill to add a definition for "sharing restriction request" under clause 2; and a new division 3A in the Bill in order to stipulate the spirit of fostering HCRs' choice over data sharing in the Bill, but at the same time not pre-empting the future design of the relevant feature.[3]	Draft CSAs proposed by the Administration, which according to the Administration, was agreeable to the Privacy Commissioner, are in Annex I.
(b) There was a question from members as to whether clause 12(6) as presently drafted	(b) While the issue of withholding otherwise sharable data in the System would be	

[2] Please refer to paragraphs 9 to 11 of LC Paper No. CB(2)1580/13-14(03), pages 4-7 of LC Paper No. CB(2)2045/13-14(01) and LC Paper No. CB(2)436/14-15(01) for details of the Privacy Commissioner's views.

[3] Please refer to item (a) of LC Paper No. CB(2)404/14-15(02) and item (ii) of LC Paper No. CB(2)808/14-15(02) for details of the Administration's response.

Views from members and/or the Privacy Commissioner for Personal Data	The Administration's latest position	Draft Committee Stage amendments to the Bill
would render it not viable for HCRs to request prescribed HCPs and referral HCPs to which they had given a sharing consent, not to provide to the System certain parts of their health data within the sharable scope.	addressed in the above study, it should be noted that clause 12(6) as presently drafted did not preclude HCRs from making requests for withholding particular data. Whether such request would/could be entertained was a matter to be considered by the HCP concerned, depending on the professional clinical judgment of the relevant healthcare professionals, the particular clinical workflow of the HCP concerned, and whether the local electronic medical record ("eMR") system of that HCP was technically capable of doing so.[4]	
Clauses 17 and 20 - Application by HCPs for registration and registration of Government bureaux and departments as HCPs		
Clause 17(5)(g) provided that an HCP provided healthcare at one service location if the HCP concerned was a specified entity that, in the opinion of the Commissioner for the Electronic Health Record ("the Commissioner"), directly or indirectly provided healthcare to any HCR at one premises. The HCP concerned might apply to the Commissioner to be registered as an HCP for the System for that location. Clause 20(1) provided that the Commissioner might register a Government bureau or department as an HCP for the System if the Commissioner was satisfied that the operation of the bureau or department involved providing	(a) Subject to members' views, the Administration would introduce CSAs to delete clause 17(5)(g). (b) Clause 20 was drafted mainly to cater for Government departments which would provide healthcare to detainees, such as the Immigration Department and the Correctional Services Department. Subject to members' views, the Administration would introduce CSAs to amend the clause to subject Government departments to similar criteria on the provision of healthcare as required of	Draft CSAs proposed by the Administration are in Annex II.

[4] Please refer to item (b) of LC Paper No. CB(2)404/14-15(02) for details of the Administration's response.

Views from members and/or the Privacy Commissioner for Personal Data	The Administration's latest position	Draft Committee Stage amendments to the Bill
healthcare. The Privacy Commissioner and some members were concerned that the above arrangements were too loose which would in effect widen the sharing of the HCR's eHR. They suggested that clauses 17(5)(g) and 20 should be deleted. In addition, the definition of "specified entity" under clause 17(6) should be expanded to subject Government bureaux or departments to similar criteria on the provision of healthcare as required of other HCPs for registration for eHRSS under clause 17(5)(f).[5]	other HCPs for registration for eHRSS under clause 17.[6]	
Proposed new clause 35A: Prescribed HCP's duty to restrict access to sharable data		
The Privacy Commissioner and some members were of the view that the cardinal principle that access to eHR in the System by individual healthcare professionals would only be made on a "need-to-know" basis should be expressly spelt out in the Bill. It was suggested that a provision should be added in the Bill to the effect that among the staff employed by a prescribed HCP with sharing consent, only relevant healthcare professionals could have access to the relevant parts of eHR kept in the System.[7]	The "need-to-know" principle had been adopted in the design of the System, and reflected in the relevant legislative provisions and system operation or workflows. This notwithstanding, the Administration would introduce CSAs to add a new clause 35A to address the concerns raised by the Privacy Commissioner and members.[8]	Draft CSAs proposed by the Administration, which according to the Administration, was agreeable to the Privacy Commissioner, are in Annex III.

[5] Please refer to paragraph 12 of LC Paper No. CB(2)1580/13-14(03) and pages 7 and 8 of LC Paper No. CB(2)2045/13-14(01) for details of the Privacy Commissioner's views.

[6] Please refer to paragraphs 29 to 31of LC Paper No. CB(2)1775/13-14(02) for details of the Administration's response.

[7] Please refer to paragraphs 7 to 9 of LC Paper No. CB(2)1580/13-14(03), pages 3 and 4 of LC Paper No. CB(2)2045/13-14(01), LC Paper Nos. CB(2)2317/13-14(01) and CB(2)436/14-15(01) for details of the Privacy Commissioner's views.

[8] Please refer to item (iii) of LC Paper No. CB(2)1775/13-14(02), Annex to LC Paper No. CB(2)2308/13-14 (02) and item (i) of LC Paper No. CB(2)808/14-15(02) for details of the Administration's response.

Views from members and/or the Privacy Commissioner for Personal Data	The Administration's latest position	Draft Committee Stage amendments to the Bill
Clause 38: Access to and correction of data or information		
Pursuant to section 17A of the Personal Data (Privacy) Ordinance (Cap. 486) ("the Privacy Ordinance"), a person authorized in writing by the data subject could make a data access request or data correction request on behalf of the data subject. Clause 38 specifically excluded the application of section 17A of the Privacy Ordinance to eHR kept in the System. The Privacy Commissioner objected to clause 38, as rights to data access or data correction were crucial for the protection of individuals' personal data. Clause 38 would also give rise to an inconsistent treatment of health data under the Bill and the Privacy Ordinance which would cause confusion.[9]	The Administration was open to views as to whether clause 38 should be retained or removed. Subject to members' views, it would introduce CSAs to delete clause 38 and the related clause 37(2)(a).[10]	Draft CSAs proposed by the Administration are in Annex IV.
Clause 41: Offences relating to accessing, damaging or modifying data or information		
Unauthorized access by non-computer means		
(a) Pursuant to clause 41(1), it would be an offence if a person knowingly caused a computer to perform a function so as to obtain unauthorized access to data or information contained in an eHR. The Privacy Commissioner considered that unauthorized access by means other than the use of a computer should also be an offence.	(a) Access to the System was mainly through computers. Unauthorized access to an eHR alone by non-computer means was not a premeditated act. To criminalize the mere act of "unauthorized access" not followed by any malicious act could arguably be disproportionate.	Nil

[9] Please refer to paragraphs 13 to 15 of LC Paper No. CB(2)1580/13-14(03) and pages 8 and 9 of LC Paper No. CB(2)2045/13-14(01) for details of the Privacy Commissioner's views.

[10] Please refer to item (vi) of LC Paper No. CB(2)1775/13-14(02) and Annex to LC Paper No. CB(2)2308/13-14 (02) for details of the Administration's response.

Views from members and/or the Privacy Commissioner for Personal Data	The Administration's latest position	Draft Committee Stage amendments to the Bill
(b) During the public consultation for the review of the Privacy Ordinance in 2010, 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.[11]	(b) Data not directly obtained from the System should not be governed by any offence provision under the Bill. At present, the mere act of accessing one's personal data without consent was not an offence under the Privacy Ordinance. If it was considered that unauthorized access of personal data without subsequent malicious act in general should be criminalized, amendments should be made to the Privacy Ordinance.[12]	
Misuse of eHR data in general		
(a) The Privacy Commissioner proposed that 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 sensitivity of health data. In particular, the person misusing the data could be different from the person making the unauthorized access in the first place. (b) Section 64(1) of the Privacy Ordinance provided that it was an offence for a person to disclose any personal data of a data subject	(a) It might not be appropriate to impose an offence on misuse of eHR in general, as there were different extents and various scenarios of "misuse" which carried a broad meaning. In addition, it was debatable whether all "misuses" should be penalized or even criminalized. (b) Misuse of personal data was generally governed by the Data Protection Principle ("DPPs") under the Privacy Ordinance. In particular, contravention of DPP3 was not an offence unless the data user failed to comply with the relevant enforcement notice issued	Nil

[11] Please refer to paragraph 16 of LC Paper No. CB(2)1580/13-14(03) and pages 9 and 10 of LC Paper No. CB(2)2045/13-14(01) for details of the Privacy Commissioner's views.
[12] Please refer to paragraphs 34 to 36 under item (vii) of LC Paper No. CB(2)1775/13-14(02) for details of the Administration's response.

Views from members and/or the Privacy Commissioner for Personal Data	The Administration's latest position	Draft Committee Stage amendments to the Bill
which was obtained from a data user without the data user's consent if certain conditions were fulfilled. Its application to small HCPs was further limited where the wrongdoer was the data user and hence, the issue of consent would not arise.[13]	by the Privacy Commissioner. While making contravention of a DPP an offence was proposed in the public consultation for the review of the Privacy Ordinance in 2010, the proposal was not pursued as the majority view received was against it.[14]	
Penalty for unauthorized access by non-computer means and misuse of eHR data in general		
The Privacy Commissioner proposed that if the Administration considered that the criminal sanction for unauthorized access by non-computer means and misuse of eHR data was too harsh, consideration could be given to introducing other penalties. The practice in Australia where misuse of eHR could be subject to civil penalty might serve as a reference.[15]	It might not be appropriate to empower the Commissioner, a non-judicial authority, to impose monetary penalty generally on "misuses of eHR data" couched in broad terms. In addition, the imposition of a financial penalty similar to "civil penalty" in Australia was not common in the legal regime of Hong Kong.[16]	Nil
Clause 53(2): Establishment of the Electronic Health Record Research Board		
Some members suggested that the precise composition of members of the Electronic Health Record Research Board should be specified under clause 53(2) with a view to ensuring that the 10 non-ex officio members to be appointed by the Secretary for Food and Health would be drawn from various fields.	The Administration would introduce CSAs to amend clauses 53(2) to elaborate on the specific requirements for the 10 non-ex officio members of the Electronic Health Record Research Board.[17]	To be advised by the Administration.

[13] Please refer to paragraphs 17 and 18 of LC Paper No. CB(2)1580/13-14(03) and pages 11 and 12 of LC Paper No. CB(2)2045/13-14(01) for details of the Privacy Commissioner's views.
[14] Please refer to paragraphs 37 and 38 of LC Paper No. CB(2)1775/13-14(02) and paragraphs 13 to 15 of LC Paper No. CB(2)2045/13-14(03) for details of the Administration's response.
[15] Please refer to page 10 of LC Paper No. CB(2)2045/13-14(01) for details of the Privacy Commissioner's views.
[16] Please refer to paragraphs 13 and 15 of LC Paper No. CB(2)2045/13-14(03) for details of the Administration's response.
[17] Please refer to item (d) of LC Paper No. CB(2)1775/13-14(03) for details of the Administration's response.

Views from members and/or the Privacy Commissioner for Personal Data	The Administration's latest position	Draft Committee Stage amendments to the Bill
Clause 57(2): Limitation of public liability		
Clause 57(2) of the Bill stipulated that the Commissioner was not obliged to inspect, or commit to inspect, an eMR system to ascertain (a) whether the ordinance was complied with; or (b) whether any sharable data provided to the System was accurate. The Privacy Commissioner objected to this provision, as it called in question how the Commissioner could exercise the supervisory and oversight role effectively. The provision would also reduce the Privacy Commissioner's enforcement power that might be invoked against the Commissioner to ensure the latter's compliance with the Privacy Ordinance. In addition, ensuring the integrity of eHR in the System was the obligation of the Commissioner as a data user under DPP4 and DPP(2)1 of the Privacy Ordinance.[18]	The Administration advised that, subject to members' views, it would introduce CSAs to delete clause 57(2).	Draft CSAs proposed by the Administration are in Annex V.

Council Business Division 2
Legislative Council Secretariat
5 March 2015

[18] Please refer to paragraphs 19 to 25 of LC Paper No. CB(2)1580/13-14(03) and pages 12 to 15 of LC Paper No. CB(2)2045/13-14(01) for details of the Privacy Commissioner's views.

Annex I

Draft Committee Stage amendments to the Bill in relation to registered healthcare recipients' choice over data sharing[1]

(Note: The proposed amendments are marked in *italic and underline type* or with deletion line)

Add a definition for "sharing restriction request" under clause 2

2. Interpretation

(1) In this Ordinance—

……

Sharing restriction request *(互通限制要求) means a request made under section 16A(1)(a);*

Add a new subclause (3)(e) and new subclauses (5)(g) and (h) under clause 3

3. Substitute decision maker

……

(3) For a healthcare recipient who is aged 16 or above and who is of any of the following descriptions, the persons specified in subsection (4) are eligible persons for the purposes of subsection (1)—

……

(d) being incapable of giving a sharing consent at the time referred to in paragraph (d), (e) or (f) of the definition of ***relevant time*** in subsection (5)~~.~~*;*

(e) being incapable of making a sharing restriction request at the time referred to in paragraph (g) or (h) of the definition of ***relevant time*** *in subsection (5).*

……

(5) In this section—

relevant time (有關時間) means—

……

(f) in relation to a sharing consent that is revoked under section 15(1), the time at which the revocation of the sharing consent is made~~.~~*;*

(g) in relation to a sharing restriction request that is made under section 16A(1)(a), the time at which the request is made;

(h) in relation to a request to remove a restriction that is made under section 16A(1)(b), the time at which the request is made.

[1] The Administration has advised that the new provisions will be arranged to take effect only upon completion of the future study on enhancing registered healthcare recipients' choice and after such feature enabling additional choice for registered healthcare recipients over the disclosure of their data is technically ready.

Add a new Division 3A

Division 3A—Sharing Restriction

16A. Request for sharing restriction

(1) Subject to subsections (2) and (3), a registered healthcare recipient, or a substitute decision maker of a registered healthcare recipient, may make – (a) a request to restrict the scope of data sharing; or (b) a request to remove a restriction on the scope of data sharing, in relation to the health data of the healthcare recipient.

(2) If the healthcare recipient is a minor, the request must be made by a substitute decision maker of the healthcare recipient unless the Commissioner is satisfied that the recipient is capable of making the request.

(3) If the healthcare recipient is aged 16 or above and is incapable of making the request, the request must be made by a substitute decision maker of the healthcare recipient.

(4) A request made by a substitute decision maker of a registered healthcare recipient is made on behalf of and in the name of the recipient.

(5) In making a request, a substitute decision maker of a registered healthcare recipient must have regard to the best interests of the recipient in the circumstances.

(6) A request must be made to the Commissioner in the form and manner specified by the Commissioner.

(7) The Commissioner must notify the requestor in writing of the date on which the requested restriction, or the requested removal of restriction, takes effect.

16B. Commissioner to specify sharing restriction

(1) The Commissioner must specify the types of restrictions in respect of which a person may make a request under section 16A(1).

(2) The Commissioner must make copies of a document setting out the specified types of restrictions available to the public (in hard copy or electronic form).

Annex II

Draft Committee Stage amendments to the Bill in relation to application by healthcare providers for registration and registration of Government departments as healthcare providers

(Note: The proposed amendments are marked in *italic and underline type* or with deletion line)

Delete subclause (5)(g) under clause 17

17. Application by healthcare providers for registration

……

(5) For the purposes of this section, a healthcare provider provides healthcare at one service location if the healthcare provider—

……

(e) holds a licence issued under section 7(2)(a), or a certificate of exemption issued under section 11(2)(a), of the Residential Care Homes (Persons with Disabilities) Ordinance (Cap. 613) in respect of one residential care home for persons with disabilities, and engages a healthcare professional to perform healthcare at that home; *or*

(f) is a specified entity that engages a healthcare professional to perform healthcare at one premises~~; or~~.

~~(g) is a specified entity that, in the Commissioner's opinion, directly or indirectly provides healthcare to any healthcare recipient at one premises.~~

Amend the heading of and subclause (1) under clause 20

20. Registration of Government ~~bureaux and~~ departments as healthcare providers

(1) The Commissioner may register a Government ~~bureau or~~ department as a healthcare provider for the System if the Commissioner is satisfied that ~~the operation of the bureau or department involves providing healthcare~~ *the department provides a healthcare professional to perform healthcare for any healthcare recipient*.

(2) The reference of a department in subsection (1) does not include the Department of Health.

Annex III

Draft Committee Stage amendments to the Bill in relation to prescribed healthcare provider's duty to restrict access to sharable data

(Note: The proposed amendments are marked in *italic and underline type*)

Add a new clause 35A

35A. Prescribed healthcare provider's duty to restrict access to sharable data

(1) This section applies if a prescribed healthcare provider is given a sharing consent by a registered healthcare recipient or a substitute decision maker of a registered healthcare recipient.

(2) The healthcare provider must take reasonable steps to ensure that— (a) access to any health data of the healthcare recipient is restricted to its healthcare professional who may perform healthcare for the recipient; and (b) the access is restricted to the health data that may be relevant for performing healthcare for the recipient.

(3) However, for complying with a data access request or data correction request under Part 5 of the Privacy Ordinance, the healthcare provider is not to be treated as contravening the requirement under subsection (2) even if access to the health data is granted to a person other than the healthcare professional.

Annex IV

Draft Committee Stage amendments to the Bill in relation to access to and correction of data or information

(Note: The proposed amendments are marked with deletion line)

Delete subclause (2)(a) under clause 37

37. Privacy Commissioner's performance of functions or exercise of powers in relation to data or information

(1) If the Privacy Commissioner performs a function or exercises a power under the Privacy Ordinance in relation to data or information contained in the System, the Privacy Commissioner must do so subject to the conditions specified in subsection (2).

(2) The conditions are —

~~(a) Part 5 of the Privacy Ordinance has effect as provided under section 38;~~

……

Delete clause 38

~~**38. Access to and correction of data or information**~~

~~Part 5 of the Privacy Ordinance applies to the access to or correction of the data or information contained in the electronic health record of a registered healthcare recipient as if the definition of ***relevant person*** in section 2(1) of that Ordinance were not modified by section 17A of that Ordinance.~~

Annex V

Draft Committee Stage amendments to the Bill in relation to limitation of public liability

(Note: The proposed amendments are marked with deletion line)

Delete subclause (2) under clause 57

57. Limitation of public liability

……

~~(2) The Commissioner is not obliged to inspect, or commit to inspect, an electronic medical record system to ascertain—~~

~~(a) whether this Ordinance is complied with; or~~

~~(b) whether any sharable data provided to the System is accurate.~~