Bills Committee on
Electronic Health Record Sharing System Bill

The Administration's Response to the issues arising from the discussion at the meeting on 29 July 2014

This paper sets out the Administration's response to the issues arising from the discussion of the Bills Committee on the Electronic Health Record Sharing System (eHRSS) Bill on 29 July 2014.

(a) Authorization in writing for access to data or information contained in the electronic health record (eHR) of a registered healthcare recipient (HCR)

(i) Potential abuse by dishonest persons

2. Pursuant to section 17A and section 18 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 (DAR) on behalf of the data subject. A person authorized in writing by a HCR may therefore on behalf of the HCR make a DAR to a healthcare provider which holds personal data of the HCR.

3. When formulating the design of the eHRSS, we noted that there were concerns over the access of eHR by third parties, in particular concerns over possible malpractice of unscrupulous employers or insurance companies trying to obtain written authorization from persons seeking employment or taking out insurance policy by coercive means in order to gain access to their eHR. For example, an employer or an insurance company may, for other ulterior motives, (i) allege that access to one's eHR is a prerequisite for determining eligibility for a job position or suitability for entering into an insurance contract, or (ii) purposively put a hidden clause in a contract empowering the employer or insurance company to gain access to one's eHR, when such health information is in fact not absolutely necessary for the purpose concerned. To address these concerns, we have proposed in our public consultation document

that the future eHRSS Ordinance should apply a more stringent standard than the current Privacy Ordinance over data access. Clause 38 of the eHRSS Bill is drafted accordingly to prohibit the "authorization in writing" arrangement.

(ii) Existing safeguards against abuse

4. Whether there is any malpractice on the part of a person authorized by an individual to make a DAR depends on the facts and circumstances of a particular case. An employer may legitimately collect health data of an employee provided that the collection is for a purpose directly related to the assessment of the suitability of the employee's continuance in employment; or directly related to the employer's administration of medical or other benefits or compensation provided to the employee (paragraph 3.2.4 of the Code of Practice on Human Resource Management issued by the Privacy Commissioner for Personal Data). The Court has also taken the view[1] that there must be cases in which disclosure of medical records would quite properly and fairly be made mandatory, and in such cases, the employer's advice to the employee concerning any adverse consequence of the latter's failure to make disclosure would not of itself constitute a threat or the exertion of undue influence.

5. As stated in the Data Protection Principle 1 (DPP1) of the Privacy Ordinance, personal data shall not be collected unless the collection of the data is for a lawful purpose, necessary and adequate but not excessive. Further, personal data shall be collected by means which are lawful and fair in the circumstances of the case. In other words, if an employer or insurance company seeks to collect personal data of an individual which is more than necessary for the purpose concerned, or if such data is collected by means which are unfair, there could be contravention of DPP1. According to section 66 of the Privacy Ordinance, where an individual suffers damage (which includes injury to feelings) by reason of a contravention of a requirement under the Privacy

[1] Cathay Pacific Airways Ltd v Administrative Appeals Board and the Privacy Commissioner for Personal Data (HCAL 50/2008)

Ordinance by a data user which relates to personal data of which the individual is the data subject, the individual is entitled to compensation from the data user.

6. Where the Privacy Ordinance permits a person to be authorized in writing by an individual to make a DAR on behalf of the individual, the authorization must presumably be a valid one. An authorization obtained by threat, coercion or misrepresentation is unlikely to be a valid authorization and in such circumstances, the requirement to make a DAR under section 18(1) of the Privacy Ordinance cannot be satisfied. According to section 18(5) of the Privacy Ordinance, a person commits an offence if he, in a DAR, supplies any information which is false or misleading in a material particular.

7. Notwithstanding the existing safeguards against the making of DAR through improper obtaining of authorization from a data subject, there are views that, given the sensitivity of eHR, there should be tight restriction of access to one's eHR; hence clause 38 of the eHRSS Bill to disallow the making of a DAR by an authorized person. The Administration is open to views as to whether clause 38 should be retained or removed as it is essentially a question of striking the balance between providing more channels of access of personal data and protection of privacy of concerned HCRs.

(iii) The making of DAR / Data Correction Request (DCR) by a parent for a mentally handicapped son/daughter who is not a minor

8. At the last meeting of the Bills Committee, a member expressed concern over the difficulty for a parent to make a DAR/DCR for a mentally handicapped son/daughter who is not a minor and enquired about the role of the Guardianship Board on this matter.

9. Part IVB of the Mental Health Ordinance (Cap.136) (MHO) deals with the guardianship of mentally incapacitated persons (MIPs), and the establishment and role of the Guardianship Board. The Guardianship Board makes guardianship order by which the powers conferred on a private guardian (a relative of the MIP) or the public

guardian (Director of Social Welfare) are specified under the MHO[2]. These powers have no specific reference to the making of a DAR/DCR. Separately, under Part II of the MHO, the court is empowered to make an order regarding the management and administration of an MIP's property and affairs.

10. The Privacy Ordinance, as the overarching legislation to protect the privacy of individuals in relation to personal data, has specific provisions governing how a DAR/DCR shall be made and handled, including who can make a DAR/DCR for a data subject. Pursuant to the Privacy Ordinance, the data subject, or a relevant person[3] on behalf of the data subject, may make a DAR/DCR. For a DAR/DCR of any data or information contained in eHRSS that falls within the meaning of personal data in the Privacy Ordinance, the eHR Office, as a data user, is obliged to comply with the relevant requirements stipulated in the Privacy Ordinance.

11. In what way a parent can assist in the making of a DAR/DCR in respect of the personal data of his/her son/daughter suffering from mental illness is a general issue faced by all data users handling DARs/DCRs (the eHR Office only being one of them) and is not specific to the

---

[2] The six powers are:
- to require the person concerned to reside at a specific place;
- to bring the person concerned to a specific place and use reasonable force for the purpose;
- to require the person concerned to attend at a place and time for medical or dental treatment, special treatment, occupation, education or training;
- to consent to medical or dental treatment if the person concerned is incapable of understanding the general nature and effect of the treatment;
- to require access to the person concerned to be given to any doctor, approved social worker or other person specified in the guardianship order; and
- to hold, receive or pay a specified monthly sum for the maintenance or other benefit of the person concerned (currently maximum at HK$13,000 per month).

[3] "Relevant person", in relation to an individual (howsoever the individual is described), means-
(a) where the individual is a minor, a person who has parental responsibility for the minor;
(b) where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs;
(c) where the individual is mentally incapacitated within the meaning of section 2 of the MHO-
(i) a person appointed under section 44A, 59O or 59Q of that Ordinance to be the guardian of that individual; or
(ii) if the guardianship of that individual is vested in, or the functions of the appointed guardian are to be performed by, the Director of Social Welfare or any other person under section 44B(2A) or (2B) or 59T(1) or (2) of that Ordinance, the Director of Social Welfare or that other person.

operation of eHRSS. A parent of a mentally incapacitated son/daughter who is not a minor may not be eligible to make a DAR/DCR for the personal data of his son/daughter kept by the concerned data user. Our understanding is that a parent, unless he/she falls within the meaning of "relevant person" under the Privacy Ordinance, cannot make a DAR/DCR on his adult son/daughter's behalf if his/her son/daughter is incapable of managing his own affairs or is mentally incapacitated within the meaning of the MHO. Hence, the issue would better be tackled in the context of the Privacy Ordinance. In any case, this problem is envisaged in the context of the making of a DAR/DCR and does not affect access of the concerned eHR by healthcare providers (HCPs) with valid sharing consent for providing healthcare to the concerned HCR.

(b) Technical feasibility of eHRSS to accommodate opting out from being taken as having given a sharing consent to the Department of Health (DH) and to the Hospital Authority (HA) when giving a joining consent

12. Clause 16(1) of the eHRSS Bill stipulates that when the HCR gives a joining consent to participate in eHRSS, he/she is taken to have given a sharing consent to HA and DH as well.

13. One of the fundamental objectives of eHRSS is fostering public-private collaboration in healthcare delivery. HA and DH, being the HCPs of the public sector serving the largest number of patients, have a vast amount of health data. These data would be the essential building blocks of patients' life-long eHR, conducive to the continuity of care of the patients. Without these health data, the eHR's content may be much more flimsy and it would substantially undermine the value and benefits of joining the eHRSS. We have therefore proposed in the public consultation document on "The Legal, Privacy and Security Framework for Electronic Health Record Sharing" published in December 2011 that HCRs' consent to HA and DH shall be part and parcel of their enrolment to eHR sharing. No objection to this proposal was received during the public consultation. We have also highlighted this proposal in our PowerPoint briefing for the Panel on Health Services at its meeting on 12 December 2011. The arrangement would also facilitate the registration

process and reduce the burden on HCRs, HA and DH. The current technical design and development of eHRSS has incorporated the aforementioned arrangement having regard to the outcome of previous public consultation.

14. Per some members' suggestion at the last meeting of the Bills Committee, the Administration has looked into the technical feasibility of modifying the design of the eHRSS to accommodate special requests for the opting out from this arrangement by HCRs or their substitute decision makers. Our preliminary assessment is that the technical alteration, though not insurmountable, would require substantial work of modification such as the redesign of workflows, modification of system design and logics as well as the programmes and applications involved. Since participation in eHRSS is voluntary, the participating HCRs should be well aware of the benefits of record sharing between public and private HCPs. The experience of the Public Private Interface-Electronic Patient Record also reflects the popularity of access to HA's record. We therefore have doubts on the merits of altering this basic design. We estimated that it would take no less than 12 months to complete. In any event, we do not envisage that the opt-out arrangement, even if it is decided to be implemented, would be technically available in the initial months of operation of eHRSS. We would wish to reiterate that whilst the opt-out arrangement is not technically infeasible, it is highly undesirable from policy perspective as it is not conducive to the realization of the objective of eHRSS as explained above.

(c) Draft proposed amendments to the bill

15. The initial draft proposed amendments proposed by the Administration are marked in revision mode on an extract of the bill at **Annex**. These draft amendments might be refined subject to views of members and further discussion with the Department of Justice.

Food and Health Bureau
September 2014

<u>Annex</u>

Electronic Health Record Sharing System Bill

– Initial Draft Amendments proposed by the Administration

(Note: Initial draft amendments are marked in red on the following extract of the draft bill)

17. Application by healthcare providers for registration

(1) A healthcare provider that provides healthcare at one service location may apply to the Commissioner to be registered as a healthcare provider for the System for that location.

(2) A healthcare provider that provides healthcare at more than one service location may apply to the Commissioner to be registered as a healthcare provider for the System for those locations as provided in subsection (3).

(3) For the purposes of subsection (2), a healthcare provider may apply for—

(a) a single registration for all of the locations; or

(b) a separate registration for each location that the healthcare provider chooses to register.

(4) An application—

(a) must be made in the form and manner specified by the Commissioner; and

(b) must be accompanied by the information specified by the Commissioner.

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

(a) is registered under section 3(4) of the Hospitals, Nursing Homes and Maternity Homes Registration Ordinance (Cap. 165) in respect of one hospital or one maternity home;

(b) is registered under section 5(2) of the Medical Clinics Ordinance (Cap. 343) in respect of one clinic;

(c) carries on the business of dentistry under section 12 of the Dentists Registration Ordinance (Cap. 156) at one premises;

(d) holds a certificate of exemption issued under section 7(2), or a licence issued under section 8(2)(a), of the Residential Care Homes (Elderly Persons) Ordinance (Cap. 459) in respect of one residential care home, and engages a healthcare professional to perform healthcare at that home;

(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.~~

(6) In subsection (5)—

specified entity (指明實體) means—

(a) an individual;

(b) a company;

(c) a partnership;

(d) a statutory body;

(e) a body corporate other than a company; or

(f) a society, or a branch of a society, registered under section 5A(1), or exempted from registration under section 5A(2), of the Societies Ordinance (Cap. 151).

****

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.

****

35. Prescribed healthcare provider's duties on electronic medical record system

A prescribed healthcare provider must take reasonable steps to ensure that the healthcare provider's electronic medical record system does not impair the security or compromise the integrity of the System.

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 access to any health data of the healthcare recipient may only be granted to its healthcare professional who performs 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.

****

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;~~

(b) a word or an expression used in this Part, and defined or otherwise explained in section 2 of the Privacy Ordinance, has the same meaning as in that section; and

(c) despite paragraph (b), a reference to a minor in the Privacy Ordinance is a reference to a person below 16 years of age.

(3) Subsection (2)(b) does not apply to the word "Commissioner".

~~**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.~~

****