Bills Committee on
Electronic Health Record Sharing System Bill

The Administration's Response to the issues arising from the discussion at the meeting on 11 November 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 11 November 2014.

(a) Study on additional access control for sensitive data

2. As explained previously, "safe deposit box" is used to describe a broad general concept. It is not a jargon with commonly accepted definition or a standard technical design. Those countries with their respective eHR sharing arrangements in place are allowing different extents of control to access to records. In this regard, the means or the extent of choice available to healthcare recipients (HCRs) to restrict disclosure of data varies from country to country.

3. We have previously undertaken to conduct a study on additional access control for sensitive data as a priority for the Stage 2 Electronic Health Record (eHR) Programme after passage of the eHRSS Bill. Views on the subject are diverse as reported in our previous written and verbal responses. In response to the comment of the Privacy Commissioner for Personal Data and some members, we have indicated at the meeting of the Bills Committee on 11 November 2014 that we will conduct the study along a positive direction, with a view to developing and implementing some form of new device/arrangement enabling additional choice for HCRs over the disclosure of their data.

4. The study will compile important background information and analyse various options to formulate possible new features to be added in the local context. It would be conducted as soon as possible after passage of the bill. Upon the completion of the study, we will consult relevant stakeholders including patient groups, professional groups and the Legislative Council on the recommended proposal.

5. The bill is technology-neutral. It is not a system manual and will not describe or prescribe system design or architecture. The current provisions of the bill do not preclude the future provision of some form of "safe deposit box" function, i.e. some new device/arrangement enabling additional means for HCRs to exercise choice or restriction over disclosure of their data.

(b) Request by an HCR that a prescribed healthcare provider (HCP) which has previously obtained his/her sharing consent not to provide certain parts of his/her sharable data to eHRSS

6. At the last meeting of the Bills Committee, there was a question on whether an HCR could request a prescribed HCP that had previously obtained his/her sharing consent under Clause 12(6) not to provide certain parts of his/her sharable data to eHRSS (the request).

7. Under the designs/workflows of the Stage 1 eHRSS and depending on the local electronic medical record (eMR) systems of prescribed HCPs, sharable data of an HCR that has been entered into the local eMR system of a prescribed HCP that has the capability to interconnect with eHRSS would be uploaded to the eHRSS. Clause 12(6) as presently drafted, do not preclude HCRs to make the request for withholding particular data. Whether such request would/could be entertained is a matter to be considered by the concerned HCP, depending on the professional clinical judgment of the relevant healthcare professionals and the particular clinical workflow of the HCPs, as well as whether the local eMR system of the HCP is technical capable of doing so.

8. As we have undertaken at the last Bills Committee meeting, after the commencement of the Stage 1 eHRSS (which is the basic core infrastructure to enable eHR sharing), we would conduct a study with a view to developing and implementing some form of new device/arrangement enabling additional choice for HCRs over disclosure of their data. The issue of withholding otherwise sharable data to eHRSS will be addressed in the aforementioned study.

(c) Comparison between the new offences proposed under the bill and the existing offences that may be applicable

9. A table setting out the six new offences proposed under Clauses 41-46 of the bill and the existing offences that may be applicable, with notes on their comparison, is at **Annex**.

Food and Health Bureau
December 2014

Annex

Comparison table on the new offences proposed under the Electronic Health Record Sharing System (eHRSS) Bill and the existing offences that may be applicable

Note: The following is for illustrative purpose only. The applicability of any offence is subject to the facts and circumstances of each individual case.

New offence(s) proposed under eHRSS Bill	Existing offences that may be applicable	Remarks
Clause 41(1)-(3) (Offence relating to obtaining unauthorised access to data or information) Act Knowingly causes a computer[1] to perform a function so as to obtain unauthorized access[2] to data or information in an electronic health record Penalty Liable on summary conviction to a fine at level 6 ($50,001 to $100,000)	**Telecommunications Ordinance (Cap. 106) – Section 27A (Unauthorized access to computer by telecommunications)** Act By telecommunications[3], knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer Penalty Liable on conviction to a fine at level 4 ($10,001 to $25,000)	The offence under Clause 41(1)-(3) is specifically directed at "data or information in an electronic health record" (as opposed to "any program or data held in a computer" generally). The offence under Clause 41(1)-(3) covers any act of "causing a computer to perform a function" instead of being confined to the act of "causing a computer to perform a function by telecommunications". The offence under Clause 41 has a higher maximum penalty.

[1] A computer means a device for storing, processing or retrieving data or information.

[2] Access by a person to data or information is unauthorized if—
(a) the person is not entitled to control that access;
(b) the person has not been authorized by another person who controls that access to obtain that access;
(c) the person does not believe that the authorization has been given; and
(d) the person does not believe that, even if the person had applied to the appropriate authority, the authorization would have been given.

[3] "Telecommunications" (電訊) means "any transmission, emission or reception of communication by means of guided or unguided electromagnetic energy or both, other than any transmission or emission intended to be received or perceived directly by the human eye".

New offence(s) proposed under eHRSS Bill	Existing offences that may be applicable	Remarks
<u>Clause 41(6)-(8) (Offence relating to accessing, modifying or impairing data or information with criminal or dishonest intent)</u> <u>Act</u> Knowingly - (i) causes access to an electronic health record; (ii) causes modification of data or information in an electronic health record; or (iii) causes impairment to the accessibility, reliability, security or process of an electronic health record; and causes the access, modification or impairment – (i) with intent to commit an offence; (ii) with a dishonest intent to deceive; (iii) with a view to dishonest gain[4] for themselves or for another; or (iv) with a dishonest intent to cause loss[4] to another whether on the same occasion as the person causes the access, modification or impairment or on any future occasion <u>Penalty</u> Liable on conviction on indictment to imprisonment for 5 years	**<u>Crimes Ordinance (Cap. 200) – Section 161 (Access to computer with criminal or dishonest intent)</u>** <u>Act</u> Obtains access to a computer- (a) with intent to commit an offence; (b) with a dishonest intent to deceive; (c) with a view to dishonest gain[5] for himself or another; or (d) with a dishonest intent to cause loss[5] to another whether on the same occasion as he obtains such access or on any future occasion <u>Penalty</u> Liable on conviction upon indictment to imprisonment for 5 years	The act to be criminalised under Clause 41(6)-(8) is broader to cover not only “access” but also “modification” and “impairment to the accessibility, reliability, security or process”. The offence under Clause 41(6)-(8) is specifically directed at “data or information in an electronic health record” (as opposed to “computer” generally).

[4] A reference to gain includes (i) a gain in money or other property; (ii) a temporary gain or permanent gain; (iii) a gain by keeping what one has; and (iv) a gain by getting what one has not.
A reference to loss includes (i) a loss in money or other property; (ii) a temporary loss or a permanent loss; (iii) a loss by getting what one might get; and (iv) a loss by parting with what one has.

[5] "gain" (獲益) and "loss" (損失) are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and-
(a) "gain" (獲益) includes a gain by keeping what one has, as well as a gain by getting what one has not; and
(b) "loss" (損失) includes a loss by not getting what one might get, as well as a loss by parting with what one has.

New offence(s) proposed under eHRSS Bill	Existing offences that may be applicable	Remarks
Clause 41(4)-(5) (Offence relating to damaging data or information) Act Without lawful excuse, knowingly damages data or information contained in an electronic health record Penalty Liable on summary conviction to imprisonment for 2 years **Clause 42 (Offence relating to impairment to System)** Act Knowingly impairs the operation of the System Penalty Liable on conviction on indictment to imprisonment for 10 years	**Crimes Ordinance (Cap. 200) – Section 60(1) (Destroying or damaging property)** Act Without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged Penalty Liable on conviction upon indictment to imprisonment for 10 years	The offences under Clause 41(4)-(5) and Clause 42 are more specifically directed at "data or information in an electronic health record" and the eHRSS respectively (as opposed to "property" generally).

New offence(s) proposed under eHRSS Bill	Existing offences that may be applicable	Remarks
<u>Clause 43 (Offence relating to data access requests and data correction requests)</u> <u>Act</u> With intent to evade a data access request or data correction request in relation to any data or information in an electronic health record – (a) alters, falsifies, conceals or destroys the data or information; or (b) directs another person to do anything mentioned in paragraph (a) <u>Penalty</u> Liable on summary conviction to a fine at level 6 ($50,001 to $100,000)	**<u>Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) – Section 64A (Miscellaneous offences)</u>** <u>Act</u> A data user who, without reasonable excuse, contravenes any requirement under the PDPO [Note: While this section does not apply to some sections of the PDPO, it does apply to Sections 19 and 23 (concerned with compliances in general with data access request and with data correction request respectively).] <u>Penalty</u> Liable on conviction to a fine at level 3 ($5,001 to $10,000)	Section 64A(1) of the PDPO is a general provision on non-compliance with the requirements under the PDPO, including those under Sections 19 and 23 (concerned with compliances in general with a data access request and with a data correction request respectively). Meanwhile, the offence under Clause 43 of the eHRSS bill is directed at non-compliance of a data access request or a data correction request specifically by way of tampering with the data or information contained in an electronic health record. The offence under Clause 43 carries a higher maximum penalty.

New offence(s) proposed under eHRSS Bill	Existing offences that may be applicable	Remarks
Clause 44 (Offence relating to untrue statements) Act Knowingly makes an untrue statement to enable the person to give a joining consent or sharing consent Penalty Liable on summary conviction to a fine at level 6 ($50,001 to $100,000)	N/A (no particularly comparable offence under existing laws)	N/A (no particularly comparable offence under existing laws)

New offence(s) proposed under eHRSS Bill	Existing offences that may be applicable	Remarks
Clause 45 (Offence relating to contravening conditions for research or statistics purpose) Act Knowingly contravenes a condition imposed under Clause 32(1)(a) [Note: This refers to the conditions of approval for use of identifiable data of a healthcare recipient contained in an electronic health record for carrying out research or preparing statistics relevant to public health or public safety.] Penalty Liable on summary conviction to a fine at level 6 ($50,001 to $100,000)	N/A (no particularly comparable offence under existing laws)	N/A (no particularly comparable offence under existing laws)

New offence(s) proposed under eHRSS Bill	Existing offences that may be applicable	Remarks
Clause 46(1) – (2) (Offence relating to using data for direct marketing[6]) [7] Act Uses another person's data or information contained in an electronic health record, or a copy (in whatever format) of the data or information, for direct marketing Penalty Liable on conviction on indictment to a fine of $500,000 and to imprisonment for 3 years	**PDPO – Section 35E (Data user must not use personal data in direct marketing without data subject's consent)** Act A data user who has complied with section 35C [Note: concerned with data user taking specified actions to inform data subject] must not use the data subject's personal data in direct marketing unless— (a) the data user has received the data subject's consent to the intended use of personal data, as described in the information provided by the data user under section 35C(2)(b), either generally or selectively; (b) if the consent is given orally, the data user has, within 14 days from receiving the consent, sent a written confirmation to the data subject, confirming— (i) the date of receipt of the consent; (ii) the permitted kind of personal data; and (iii) the permitted class of marketing subjects; and (c) the use is consistent with the data subject's consent. A data user who contravenes the above commits an offence. Penalty Liable on conviction to a fine of $500,000 and to imprisonment for 3 years	Under the PDPO, personal data may be used for direct marketing if the data user has taken the specified action and has obtained the data subject's consent. The offence under Clause 46(1)-(2) of the eHRSS bill provides that data and information contained in an electronic health record should not be used for direct marketing in general.

[6] "Direct marketing" has the meaning given by section 35A(1) of the PDPO.

[7] This clause does not apply in relation to the use or provision of data or information contained in an electronic health record, or a copy (in whatever format) of the data or information, by a person if, not for gain, the person uses or provides the data or information, or the copy, for a purpose of the offering, or the advertising of the availability, of—
(a) social services run, subvented or subsidized by the Social Welfare Department;
(b) healthcare services provided or administered by the Department of Health or the Hospital Authority; or
(c) any other social or healthcare services that, if not provided, would be likely to cause serious harm to the physical or mental health of (i) the individual to whom the services are intended to be provided; or (ii) any other individual.

New offence(s) proposed under eHRSS Bill	Existing offences that may be applicable	Remarks
Clause 46(3) – (4) (Offence relating to providing data, for gain, to others for direct marketing[6]) [7] Act For gain, the person provides to others another person's data or information contained in an electronic health record, or a copy (in whatever format) of the data or information, for direct marketing Penalty Liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years **Clause 46(5) – (6) (Offence relating to providing data, not for gain, to others for direct marketing[6]) [7]** Act Not for gain, the person provides to others another person's data or information contained in an electronic health record, or a copy (in whatever format) of the data or information, for direct marketing Penalty Liable on conviction on indictment to a fine of $500,000 and imprisonment for 3 years	**PDPO – Section 35K (Data user must not provide personal data for use in direct marketing without data subject's consent)** Act A data user who has complied with section 35J [Note: concerned with data user taking specified actions to inform data subject] must not provide the data subject's personal data to another person for use by that other person in direct marketing unless— (a) the data user has received the data subject's written consent to the intended provision of personal data, as described in the information provided by the data user under section 35J(2)(b), either generally or selectively; (b) if the data is provided for gain, the intention to so provide was specified in the information under section 35J(2)(b)(i); and (c) the provision is consistent with the data subject's consent. A data user who contravenes the above commits an offence. Penalty Liable on conviction to (i) (if the data user provides the personal data for gain) a fine of $1,000,000 and to imprisonment for 5 years (ii) (if the data user provides the personal data otherwise than for gain) a fine of $500,000 and to imprisonment for 3 years	Under the PDPO, personal data may be provided to another person for use for direct marketing if the data user has taken the specified action and has obtained the data subject's consent. The offences under Clause 46(3)-(6) of the eHRSS bill provide that data and information contained in an electronic health record should not be provided to another person for use for direct marketing in general, whether for gain or not for gain.

Food and Health Bureau
December 2014