Bills Committee on
Electronic Health Record Sharing System Bill

The Administration's Response to the issues arising from the discussion at the meeting on 12 May 2015

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 12 May 2015.

(a) Drafting matters concerning the offences proposed under Clause 41(6)

2. Under Clause 41(6), a person commits an offence if:

(a) the person knowingly causes (i) access to / (ii) modification of / (iii) impairment to the accessibility, reliability, security or processing of data or information contained in an electronic health record (eHR), and

(b) the person 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 for the person or for another / (iv) with a dishonest intent to cause loss to another, **whether on the same occasion as the person causes the access, modification or impairment or on any future occasion**.

The term "occasion" in Clause 41(6)(b)

3. At the meeting on 12 May 2015, a member enquired about the difference in the use of "whether on the same occasion...or on any future occasion" instead of "whether at the time…or at a future time" in the English text. He also asked to review the use of "不論是在...的同時...或是在日後任何時間..." in Clause 41(6)(b) in the corresponding Chinese text.

4. We have further looked at the issue and wish to confirm that there is no discrepancy in the legal meaning or interpretation of the

bilingual texts. Since the Chinese text is not a direct translation of the English text (and vice versa), the Chinese text is interpreted according to its own linguistic characteristics or usage. The expression "on the same occasion" is used in the legislation from time to time. It gives a necessary sense of a "space of time" for the concerned act to be done with the intent. By comparison, it is more restrictive to use "at the same time" than "on the same occasion" in the English text.

5. On the other hand, if we use "同一事件中" in the Chinese text, it might cover a much longer span of time than what is intended. We consider the current Chinese rendition reflects the policy intent as much as the English text does. In addition, Clauses 41(6)(b) of our bill were drafted with essentially the same wording as that of Section 161(1) of the Crimes Ordinance (Cap. 200). The intention was to maintain consistency on the required criminal/dishonest intent in providing for the new offence in Clause 41(6) specifically directed at "data or information in an eHR" (as opposed to "computer" generally) and criminalizing "modification" and "impairment to the accessibility, reliability, security or processing" in addition to "access" in relation to the data or information. Such consistency in wording is considered necessary because we should maintain a consistent approach in prosecuting cases with similar elements.

<u>The term "any" in Clause 41(6)(b)</u>

6. At the meeting, the member enquired why "any", instead of "a", was used in "any future occasion" in Clause 41(6)(b). As aforementioned, Clause 41(6)(b) of the eHRSS Bill were drafted with essentially the same wording as that of Section 161(1) of Cap. 200 and it is necessary to maintain consistency. Apart from this consistency dimension, we have also considered it from a language perspective. Although the latest drafting convention is to avoid using "any" indiscriminately, there are indeed still circumstances in which the use of "any" is preferred to that of "a" or "an". We use "any future occasion" (instead of "a future occasion") in Clause 41(6)(b) because we want to refer to any future occasion *generally*. If "***a*** future occasion" is used, the focus might be slightly switched to looking for a *particular* future occasion. The same rationale applies to the Chinese text.

Overall drafting of Clause 41(6)(b)

7. At the meeting, the member also observed that the expression "whether on the same occasion…or on any future occasion" in the English text was separately featured in brackets towards the end of each of sub-clauses (i) to (iv) of Clause 41(6)(b) in the Chinese text, and enquired whether the drafting of the Chinese text of the clause could be refined to make it more comprehensible / reader-friendly. As aforementioned, Clause 41(6)(b) was drafted with essentially the same wording as that of Section 161(1) of Cap. 200 and it is necessary to maintain consistency. Apart from this consistency dimension, owing to its respective linguistic characteristic, different sentence structure has been used in the English and the Chinese texts. In this case, the expression "whether on the same occasion…or on any future occasion" relates to a time element which qualifies the intended actions under sub-clause (i) to (iv). As different action words have been used in sub-clause (i) to (iv), in order to qualify the respective intended action with the time element in the Chinese text, the time element has to be immediately followed by the particular action word e.g. "同時犯罪…日後任何時間犯罪".

(b) The power of the eHR Commissioner (eHRC) to require production of records or documents in certain circumstances as provided under Clause 50

8. Clause 50(1) provides that if it appears to eHRC that there are circumstances suggesting the happening of an event specified in subsection (2), eHRC may in writing require a **registered healthcare provider (HCP)** to produce the record or **document** (a) that is or may be relevant to the event and (b) that is **in the HCP's possession**.

Definition of "document" in Clause 50(1)

9. As explained in our letter dated 23 February 2015 to the Assistant Legal Advisor (ALA) (vide LC Paper No. CB(2)911/14-15(01)) and elaborated at the meeting on 12 May 2015, Section 3 of the Interpretation and General Clauses Ordinance (Cap. 1) has already

provided that "document" (文件) means "any publication and any matter written, expressed or described upon any substance by means of letters, characters, figures or marks, or by more than one of these means". Such definition does not preclude documents in the electronic format. In the absence of a specific definition in an ordinance, the interpretation of the term "document" will follow the definition of the term in Cap. 1.

10. A specific definition of the term "document" is necessary if it is considered that the meaning given by Cap. 1 cannot reflect the policy intent in a specific context. At the meeting on 12 May 2015, the ALA and a member suggested that we better provide expressly in the bill that the term "document" in Clause 50(1) would cover "electronic document" to minimize the risk of misinterpretation. Having regard to the aforementioned consideration and the context of our bill, we do not consider it necessary to define "document" under our bill. We maintain the view that it is not necessary to do so.

11. As for the two examples mentioned by the ALA at the meeting (i.e. the Copyright Ordinance (Cap. 528) and the Unsolicited Electronic Messages Ordinance (Cap. 593)), we would like to point out that there is in fact no definition of "document" in the former while the latter has a specific context not shared by our bill and not a suitable reference. In this connection, Members may wish to note that the term "document" is also not defined in the Electronic Transactions Ordinance (Cap. 553) although the Ordinance deals with electronic transactions. Indeed, out of a search of more than 450 local legislations, only about 20 enactments contain a definition of "document". Examples include the Land Registration Ordinance (Cap. 128) (which defines the term to include "any map, plan or drawing etc."); the Education Ordinance (Cap. 279) (which defines the term to include "any account, counterfoil, text-book, exercise book etc.); and the Companies (Winding Up and Miscellaneous Provision) Ordinance (Cap. 32) (which defines the term to include "summons, notice, order and other legal process etc."). On these examples, there are some obvious needs for giving a specific definition for "document". However, we have yet to see any such obvious reasons to include a specific definition of the term in our bill.

The condition "in the HCP's possession" in Clause 50(1)(b)

12. At the meeting, a member has suggested that we amend the clause concerning record or document that eHRC could require an HCP to provide in the context of Clause 50(1)(b). Having regard to the suggestion, we are prepared to propose an amendment to expand the scope to cover record or document "in the possession or under the HCP's control", the draft of which is marked in revision mode at **Annex A**. It may be further refined subject to discussion with the Department of Justice (DoJ).

The Hospital Authority (HA) and the Department of Health (DH)

13. At the meeting, the ALA and Chairman also suggested that we subject HA and DH, in addition to registered HCPs, to the requirement to produce records or documents upon eHRC's request under Clause 50. Having regard to the suggestion, we are prepared to propose an amendment to this effect, the draft of which is marked in revision mode at **Annex A**. It may be further refined subject to discussion with DoJ.

(c) Code of Practice (CoP)

14. The eHRC may issue a CoP pursuant to Clause 51 of the bill As explained previously, the CoP is an administrative instrument for providing guidelines on best practices relating to the use of eHRSS. It is of operational nature and will help users better understand the working of the system and how to better perform certain functions, e.g. procedures to handle application for registration. It is not mandatory to follow all the recommended practices in the CoP but HCPs should be reminded of the risk of non-compliance.

15. The CoP is under preparation and will be finalised having regard to the eHRSS Ordinance to be enacted, the final workflow of the operation of the eHRSS and the comments of Steering Committee on eHR Sharing which comprises representatives of relevant stakeholders. It will be publicized before the commissioning of eHRSS. We have previously briefed members on the nature, framework and key features of the CoP at the meeting on 8 December 2014. Nevertheless, noting

members' request at the meeting on 12 May 2015, we hereby provide the preliminary English working draft to date at **Annex B** for members' reference. It should be noted that the document is prepared on a provisional basis with reference to similar guidelines issued by various authorities and renowned organisations in overseas countries where electronic medical or patient record systems have been implemented as well as the provisions in the bill as currently drafted (taking into account our draft proposed amendments thus far). It serves merely as an indication of the content of the eventual CoP in future, which can only be finalised after confirmation of the provisions of the bill and further consultation with relevant stakeholders. It will be the eHRC's duty, which should not be construed as having been affected by the document in any way, to draw up, consult on and issue its CoP after the passage of the bill.

(d) Complaint handling mechanism

16. Clause 48(h) of the bill provides that the eHRC has the function to devise a mechanism for handling complaints relating to the operation of the eHRSS. As explained in our letter dated 23 February 2015 to the ALA (vide LC Paper No. CB(2)911/14-15(01)) and elaborated at the meeting on 12 May 2015, the mechanism will be devised with reference to existing relevant guidelines of the Administration, and suitably promulgated to stakeholders when available.

17. In respect of the ALA's enquiry at the meeting whether we should stipulate in the bill the form and manner of the making and handling of complaints relating to eHRSS operation, we would reiterate that this would not be necessary. The major duty of eHRC is to operate, maintain and develop the eHRSS. His/her job nature is very different from that of the Ombudsman, the Privacy Commissioner for Personal Data or the Independent Police Complaints Council, etc. Handling complaints / conduct investigations relating to statutory / serious non-compliances in response to complaints is part of their major responsibilities. In this regard, eHRC Office's situation is more comparable to many Government departments, public bodies (such as HA and the Airport Authority), Legislative Council secretariat, etc. Their major functions are delivery of services, operation of systems/facilities,

management of resources, etc. Though they may need to handle complaints, the form and manner of the making and handling of complaints are not stipulated in the relevant ordinances (if any) of these bodies.

18. At the meeting, a member also enquired about the procedures for handling complaints relating to eHRSS operation. We have explained that the detailed mechanism will be devised with reference to existing relevant guidelines of the Administration, and suitably promulgated to stakeholders when available. The key principles and intended workflows in our draft framework are set out at **Annex C** for reference.

Food and Health Bureau
May 2015

Annex A

Proposed draft amendments
in relation to the requirement for healthcare provider to produce records or documents in certain circumstances

(Note: Draft amendments are marked in red and with underline/strike-through on the following extract of the draft bill.)

****

50. Commissioner to require production of records or documents in certain circumstances

(1) If it appears to the Commissioner that there are circumstances suggesting the happening of an event specified in subsection (2), the Commissioner may in writing require a ~~registered~~ prescribed healthcare provider to produce the record or document—

(a) that is or may be relevant to the event; and

(b) that is in the ~~healthcare provider's~~ possession or under the control of the healthcare provider.

(2) The event is that—

(a) the healthcare provider contravenes—

(i) a provision of this Ordinance;

(ii) a provision of a code of practice issued under section 51; or

(iii) a condition for the registration;

(b) the healthcare provider no longer provides healthcare at the service location to which the registration relates;

(c) the healthcare provider no longer complies with—

(i) the requirements specified by the Commissioner for connecting the healthcare provider to the System; or

(ii) the system requirements on data sharing specified by the Commissioner;

(d) the service or business nature of the healthcare provider is no longer consistent with the purpose of the use of data and information specified in section 26; or

(e) the registration may impair the security or compromise the integrity of the System.

(3) The requirement must specify the manner in which the record or document must be produced.

****

Annex B

Code of Practice for Using eHR for Healthcare (Working Draft)

1. INTRODUCTION

1.1. PRACTCAL GUIDELINES FOR USE OF eHRSS

This Code of Practice (COP) is an administrative document issued by the Commissioner for Electronic Health Record ("the Commissioner" or "eHRC") under section XX of the Electronic Health Record Sharing System Ordinance (Cap XXX) (eHRSSO) ("the Ordinance").

This COP helps eHRSS users and participants (in particular healthcare provider's executive, administrative, technical staff and healthcare professionals) to better understand the operation of and the requirements for using Electronic Health Record Sharing System (eHRSS or the System). It sets out the major principles, standards and best practices for using eHRSS in a secure and proper manner.

This COP is for reference and it is not mandatory to comply with all the requirements and best practices set out in it. HCPs and healthcare professionals may find alternative ways other than those recommended in the COP which also enable them to meet the relevant requirements in the eHRSSO. However, not otherwise engaging in appropriate practices may lead to security or privacy incidents and put the participants at risk of not able to continue to use the system.

Mere non-compliance with this COP by itself does not render the person to any criminal proceeding unless such action of breach in itself constitutes an offence under the eHRSSO or other ordinances.

1.2. TARGET READERS

Section 2 - *COP for eHR Management Executives, Administrative and Technical Staff* provides general and practical guidance for Management Executives, Administrative and Technical Staff working in Healthcare Providers (HCPs) who have participated in the eHRSS. This part highlights the responsibilities of the healthcare staff management, administrative duties and technical set up for using eHRSS.

Section 3 - *COP for eHR Healthcare Professionals* provides general and practical guidance specific for healthcare professional. This part highlights the responsibilities and good practices for healthcare professionals in the use of eHRSS for sharing health information for providing healthcare to Healthcare Recipients (HCRs).

1.3. USE OF COP

Reading this COP facilitates understanding and compliance with the Electronic Health Record Sharing System Ordinance (eHRSSO) and other relevant ordinances to safeguard HCRs' privacy and confidentiality for using eHRSS. In compiling this COP, reference has been made to similar guidelines issued by various authorities and renowned organisations in overseas countries where electronic medical or patient record systems have been implemented.

This COP provides technical and operational guidelines and recommended best practices for participating HCPs and their healthcare staff (HCS). However, it should not be regarded as exhaustive.

Users are recommended to read this COP in conjunction with the eHRSSO (Cap XXX), PD(P)O and other references quoted in this document. Other useful references include notices, newsletters and relevant updated information issued by the eHR Office. Readers are also reminded to make reference to the Code of Practice and Guidance issued by the Office of the Privacy Commissioner for Personal Data (PCPD) regarding protection of personal data privacy.

eHRC may, from to time revise the whole or any part of this COP and publish further guidelines and other requirements for operation of the eHRSS.

2. CODE OF PRACTICE FOR MANAGEMENT EXECUTIVES, ADMINISTRATTIVE AND TECHNCIAL STAFF

2.1. REGISTRATION OF HEALTHCARE PROVIDERS IN EHRSS

2.1.1. Healthcare providers meeting the registration requirements set out in eHRSSO may apply to the eHRC for registration in eHRSS.

2.1.2. eHR healthcare providers should maintain an updated registration record , including business registration, contact persons, details of participating hospital(s) or clinic(s) and service locations…etc. They should inform eHRC timely for changes in business nature and clinical services and provide all necessary supporting information for verification. (Please refer to the *Guidelines and Procedures for Registration of HCP* for a complete checklist of the information /documents that must be submitted and the administrative procedures for registration).

2.1.3. eHR healthcare providers should withdraw from eHRSS if they no longer fulfil the registration requirements e.g. change of nature of services or termination of business.

2.1.4. eHR healthcare providers should understand and fulfil the conditions of registration for Electronic Health Record Healthcare Provider set by the eHRC.

2.1.5. eHR healthcare providers should be aware that their registration may be suspended or cancelled by eHRC due to breaching of any specified requirement set out by eHRC. Any such suspension or cancellation in registration may affect sharing of their HCRs' records in eHRSS.

2.2. HANDLING REGISTRATION OF HCR

2.2.1. eHR healthcare providers should observe the operational and administrative requirements set out by the eHR Office for registering HCRs in eHRSS. (Please refer to the *Guidelines and Procedures for HCR Registration* for registration of capable adults, minors, new-born, mentally incapacitated persons and persons incapable of giving consent and registration matters when eHRSS is notified that a HCR has died)

2.2.2. eHR healthcare providers should verify the identity of the HCR and check if the HCR holds:

(a) an HK Identity Card;

(b) a certificate of registration of birth issued underthe Births and Deaths Registration Ordinance (Cap. 174);

(c) a proof of identity as defined by section 17B(1) (other than an identity card) of the Immigration Ordinance (Cap. 115);
(d) a certificate of exemption as defined by section 17G(1) of the Immigration Ordinance (Cap. 115); or
(e) any other identification document specified by the Commissioner.

2.2.3. eHR healthcare providers should ensure accurate capture and verification of HCR's information during registration.

2.2.4. eHR healthcare providers should submit a copy to the eHR Office and retain appropriate original supporting documents for verification.

2.2.5. eHR healthcare providers should understand the conditions which would allow Substitute Decision Maker (SDM) to act for HCRs incapable of giving consent in registration and related procedures.

2.2.6. eHR healthcare providers should ensure their administrative staff handle HCRs' and/or SDM's HKIC with care and in accordance with the *Guidelines and Procedures for Using Hong Kong Identity Card (HKIC) for eHRSS* and *Guidance for Using Personal Identifier* issued by the PCPD for handling HCRs registration and consent matters.

2.2.7. eHR healthcare providers should ensure HCRs and their SDMs understand and agree with the conditions and purpose of using their personal data for registration and giving consent in relation to:
(a) Giving consent to join eHRSS;
(b) Giving sharing consent to healthcare providers; and
(c) Updating registration information (e.g. HCR withdrawing from eHRSS or revoking consent to a healthcare provider).

2.2.8. eHR healthcare providers should update demographic information of their HCRs and their SDMs and timely inform eHR Office of any amendments and update in major identification keys (e.g. HCR's Names, Sex, Date of Birth, Hong Kong Identity Card number or Other Travel Document Numbers).

2.3. OBTAIN HCR's CONSENT FOR EHR ACCESS

2.3.1. eHR healthcare providers should obtain express, informed consent from HCRs or their SDMs (if applicable) for:
(a) registration in eHRSS and
(b) sharing of their health information through the eHRSS

2.3.2. eHR healthcare providers should take the following actions to ensure HCR's or his/her SDM's consent (if applicable) is valid and well-informed by:
(a) Providing sufficient, relevant and comprehensible information (e.g.

Patient Information Notice, pamphlets, posters…etc.)

(b) Obtaining consent from SDM for HCRs who are incapable of giving consent; and

(c) Requesting the HCR or their SDM to confirm that their consent is voluntary

2.3.3. eHR healthcare providers should be aware of the general principles of handling consent by HCRs:

(a) A person can give consent to register for or withdraw from eHR sharing, and to give or revoke sharing consent unless he/she is a minor under age 16 or there is evidence that he/she is incapable of giving consent.

(b) For minors and HCR who are incapable of giving consent, consent should be given by their SDMs.

2.3.4. eHR healthcare providers should be acquainted with the types of persons eligible to act as a SDM for a particular class of HCR as stipulated by the eHRSSO, who may give a substitute consent for that class of HCR to register or withdraw from eHRSS and to give sharing consent to HCP(s). eHR healthcare providers should always respect the HCR's own expressed preference. If the HCR could clearly express his/her intent, the Healthcare Providers should carefully assess whether his/her case indeed require any SDM.

2.3.5. eHR healthcare providers should be aware that where there is no other eligible SDM available and the healthcare providers consider that it is in the best interest for the HCRs, the healthcare providers can choose to give consent for registration and sharing in the eHRSS under the Ordinance (eHR healthcare providers should appoint designated person under its charges to perform the tasks of the SDM of the HCRs).

2.3.6. eHR healthcare providers should be aware that there are two types of Sharing Consent: "Indefinite Sharing Consent" & "One-year Sharing Consent".

2.3.7. eHR healthcare providers should be aware that "Indefinite Sharing Consent' is in effect until it is revoked or the registration of the HCR is withdrawn or cancelled.

2.3.8. eHR healthcare providers should be aware that "One-Year Sharing Consent" to healthcare providers is valid for one year unless it is revoked or the registration of the HCR is withdrawn or cancelled.

2.3.9. eHR healthcare providers should not share health information of HCRs through eHRSS who have withdrawn from registration or revoked their sharing consent.

2.3.10. eHR healthcare providers should be aware that HCRs will receive a

notification from eHRSS for access to their eHR in the form chosen by the HCRs including but not limited to the following:

(a) Electronic message (e.g. Short Message Service (SMS));
(b) Postal mail; and
(c) e-mail

2.3.11. eHR healthcare providers should provide HCRs with access to their organizations' privacy policy document(s) and information about the kinds of data that will be shared and the purposes of sharing to eHRSS.

2.4. EHR HEALTHCARE PROVIDERS TO MANAGE HCS' USER ACCOUNT

2.4.1. eHR healthcare providers should be responsible for registering and maintaining their HCS' user accounts including checking and updating professionals registration status if appropriate for all healthcare professionals working in the eHRSS for validation in a timely manner according to the *Guidelines and Procedures for HCS Registration*. eHR healthcare providers should close the accounts of departing staff before their last day of service.

2.4.2. eHR healthcare providers should issue appropriate authentication means (e.g. security token), according to the guidelines issued by the eHR Office to their healthcare professionals to access eHRSS.

2.4.3. eHR healthcare providers should ensure only authorized healthcare professionals with the need to know about the health information of the HCRs for the purpose of providing healthcare can access to eHR of HCRs.

2.4.4. eHR healthcare providers should ensure their staff respect and have adequate awareness and knowledge of personal privacy, information confidentiality and system security.

2.4.5. eHR healthcare providers should ensure that their HCS are aware that using HCRs' information from eHRSS for direct marketing is forbidden.

2.4.6. eHR healthcare providers should take reasonable and practicable steps to ensure their healthcare professionals properly use security controls and devices (e.g. log-in password and security tokens).

2.4.7. eHR healthcare providers should appoint administrative and technical staff, as contact person(s) to communicate with the eHR Office.

2.4.8. eHR healthcare providers should supervise and monitor staff carrying out administrative and technical duties, including but not limited to:

(a) Registering and managing information of healthcare providers in eHRSS;
(b) Registering and managing information of HCRs in eHRSS;
(c) Registering and managing information of healthcare professionals in

eHRSS;

(d) Performing regular reporting, exceptional reporting and cooperating with eHR Office in audit on eHR operations

2.5. MANAGE HEALTHCARE PROVIDERS' OWN CLINICAL RECORDS

2.5.1. eHR healthcare providers should maintain clear and updated clinical records for their HCRs. eHR should not be taken as a replacement of a healthcare providers' own HCR records.

2.5.2. eHR healthcare providers should ensure the data in their medical record system is accurate for sharing.

2.5.3. eHR healthcare providers should share the health information of their HCRs who have consented to the sharing of their health records in eHRSS if the information is readily available and sharable after each episode of care as soon as possible .

2.6. MAKE DATA SHARING SECURED

2.6.1. eHR healthcare providers will be notified by eHR Office of the standards, policies and requirements on security and interfacing for data sharing between their eMRs or ePRs with eHRSS. eHR healthcare providers should endeavour to comply with these requests. (List of detailed requirement documents will be distributed and available for registered eHR HCPs and their relevant staff)

2.6.2. eHR healthcare providers should perform self-assessment and tests with eHR Office for data readiness and interoperability before sharing information to eHRSS according to the *eHRSS Data Interoperability Standards*.

2.6.3. eHR healthcare providers should perform system connection testing with the eHR Office for data sharing according to security requirements and other specifications according to the *eHRSS Data Requirement Specification document*.

2.6.4. eHR healthcare providers should provide amended and updated records in their eMR to eHRSS if previous records have been shared to eHRSS.

2.6.5. eHR healthcare providers should maintain relevant system audit logs about access to eHRSS through their eMR systems *according to the eHR IT Security Policy.*

2.6.6. eHR healthcare providers should perform regular monitoring and audit on system behaviour for identification of abnormality, intrusion and potential

system fault or user misbehavior.

2.6.7. eHR healthcare providers should report as soon as possible to eHR Office any suspected security incidents, privacy incidents and suspected security weakness related to using eHRSS.

2.6.8. eHR healthcare providers should perform periodic Security Risk Assessment and Audit (SRAA) of their own eMR systems or perform security assessment and fix any identified security loop holes according to the requirements specified by the eHR Office for system connection according to the *eHR Connection Mode Guide*. Any identified security risks or non-conformance with the security requirements should be rectified in a timely manner.

2.6.9. eHR healthcare providers should cooperate with eHR Office for auditing or investigations if necessary.

2.6.10. eHR healthcare providers should provide adequate security and privacy awareness training for their healthcare staff proper using of eHRSS.

2.6.11. eHR healthcare providers should implement, and maintain the implementation of, the security measures relating to the eHRSS which are prescribed from time to time by the eHR Office:

(a) Keep and access only enabled computers (i.e. with appropriate certification software) in secured physical locations (e.g. access within secured workplace, clinic or office) and avoid access to eHRSS in public areas such as internet cafe or public library;

(b) Keep and maintain security in wired and wireless network for computers connecting to eHRSS

(c) Keep computer system and software updated with latest security patches applied;

(d) Use only licensed / legal computer software and with latest security patches applied and avoid using peer-to-peer software (e.g. Foxy or Bit Torrent…etc.);

(e) Install appropriate anti-virus and anti-spyware software;

(f) Ensure staff logoff eHRSS and local EMR systems after use;

(g) Enable automatic screen-lock or screen-saver with password protection on computer workstation and set up of a reasonable idle time;

(h) Ensure staff should observe password policies (e.g. use of strong sword with regular updates, avoid writing down or sharing of password; change the eHRSS system assigned password immediately after successful login for the first time);

(i) Record and manage access rights assigned to each authorized staff according to their roles in delivering healthcare to the patients and;

(j) Assign individual account for each user and ensure them use properly any means of security log-on measures or devices (e.g. log-in password and security token) and protect them against unauthorised use (e.g. sharing with others)

2.7. HANDLING DATA ACCESS REQUEST AND DATA CORRECTION REQUEST

2.7.1. eHR healthcare providers should advise HCRs to approach eHR Office for Data Access Request for eHR data contained in eHRSS.

2.7.2. eHR healthcare providers should handle Data Correction Request in accordance with the relevant provisions in PD(P)O and eHRSSO.

2.7.3. eHR healthcare providers should be aware that Data Correction Request for *demographic* data (e.g. Name, Identity Number, Date of Birth or Sex) in eHRSS can be handled by both eHR Office or a prescribed eHR HCP

2.7.4. eHR healthcare providers should be aware that Data Correction Request for the HCRs' *clinical data* in the eHRSS should be reviewed by the healthcare providers who have contributed and shared that information to eHRSS according to established workflow for handling of such requests by the eHR Office. (*Policy and Guidelines for Handling DAR & DCR in eHRSS*)

2.7.5. eHR healthcare providers should update and provide corrected clinical records to the eHRSS as soon as possible once an error of their HCR's record is noted and rectified.

2.7.6. eHR healthcare providers should exercise careful judgement to handle the data correction request and to inform the HCRs and eHR Office the result of such requests and the reason of refusal if the request is refused.

2.7.7. eHR healthcare providers should make a note and attach a note to the HCR's record and provide to eHRSS if the Data Correction Request is refused and the data to which it relates is an expression of opinion according to the PD(P)O.

3. CODE OF PRACTICE FOR HEALTHCARE PROFESSIONALS

3.1. MAINTAINING USER ACCOUNT

3.1.1. eHR healthcare professionals will be provided a user account in eHRSS through the healthcare provider(s) they work with.

3.1.2. eHR Healthcare professionals should provide the eHRSS with updated professional registration information.

3.2. UPDATE RECORDS FOR EHR SHARING

3.2.1. eHR healthcare professionals should keep clear, accurate and updated clinical records of their HCR and share to eHRSS in a timely manner.

3.2.2. eHR healthcare professionals should comply with PD(P)O in collecting information in their HCRs' records and make sure it is accurate and not excessive.

3.2.3. eHR healthcare professionals should advise HCRs to approach the original HCP who provide the specific information to eHRSS for data correction if they notice any genuinely incorrect information in their eHR which is provided by other HCPs or healthcare professionals. It is advisable to document such observation in their HCRs' records.

3.2.4. eHR healthcare professionals should have duty and responsibility to assist their respective healthcare providers to deal with any data correction request for any alleged incorrect information in their HCRs' clinical records that has been shared to eHRSS in a manner and within a time frame as specified under PD(P)O.

3.2.5. eHR healthcare professionals should exercise careful judgment for accepting or refusing a data correction request from their HCRs. If they are not satisfied that the information to which the request relates is inaccurate and they should inform HCRs or the data requesters the decision and reasons of refusal.

3.2.6. eHR healthcare professionals should document the reasons for refusal for data correction request in their HCR's records and inform eHR Office if the data in dispute is an expression of opinion in accordance with the PD(P)O

3.3. POINTS TO NOTE WHEN ACCESSING A HCR'S EHR

3.3.1. eHR healthcare professionals should ensure their access to a HCR's eHR is under authorisation and with the need to know for the purpose of providing healthcare to the HCR.

3.3.2. eHR healthcare professionals should have the responsibility to exercise judgement on clinical grounds on whether and how much information from a HCR's eHR should be accessed for reference purposes.

3.3.3. eHR healthcare professionals should have the autonomy and professional judgment to interpret the information on eHRSS.

3.3.4. eHR healthcare professionals should access only to the HCRs' eHR, from whom a valid consent has been obtained. As a matter of good practice, it is advisable for healthcare professionals to inform their HCRs their eHR is to be accessed. In any event, after each access the HCRs will be notified by the system of the access.

3.3.5. eHR healthcare professionals are advised to inform their HCRs that access to their eHR beyond usual consultation time is possible for valid reasons (e.g. before-clinic visit preparation or after-clinic follow-up care).

3.3.6. eHR healthcare professionals should be aware that each access will be subject to audit and HCRs or their SDM will be notified about access to their eHRs.

3.3.7. eHR healthcare professionals should be aware that, for any HCR who is incapable of giving sharing consent to healthcare providers for eHR access, the healthcare professionals may gain emergency access to the eHR of the HCR if that is of paramount importance for provisions of emergency treatment to the HCR. eHR healthcare professionals are advised to document such access in their HCRs' record and the justification in the eHRSS and should be aware that such emergency access is subject to audit.

3.4. POINTS TO NOTE WHEN VIEWING AND USING EHR

3.4.1. eHR healthcare professionals should interpret information from eHRSS with care as it may not be updated and complete. They should judge there is a need to verify with other sources of information, and ideally, with the HCR, especially when in doubt or inconsistency is noted.

3.4.2. eHR healthcare professionals should not regard eHR as a substitute for personal communication with their HCRs and other healthcare professionals.

3.4.3. eHR healthcare professionals should record and document relevant important decisions and discussions with their HCRs based on the information from eHRSS (including date / time of information being created and accessed,

significant findings and conclusion after discussion with HCRs. . .etc.).

3.4.4. eHR healthcare professionals should be aware that they have no obligation to copy all information from the eHRSS into their own HCRs' records.

3.4.5. eHR healthcare professionals should clearly indicate the source of information, date / time of the information being accessed when copying information from eHRSS in their own HCRs' records.

3.4.6. eHR healthcare professionals should not use information from eHRSS for writing reports for third parties (e.g. insurance claims or health check report). Reports for third parties should be based on the healthcare professionals' own clinical records and/or assessment of the HCRs.

3.4.7. eHR healthcare professionals should exercise diligence of care in explaining any information accessed through eHRSS to HCRs and not to use them for alleging challenges or criticism in whatever means to depreciate the professional skills, knowledge services or qualification of other healthcare professionals and/or healthcare providers.

3.5. RESPECT CONFIDENTIALITY OF HCR'S INFORMATION

3.5.1. eHR healthcare professionals should respect confidentiality of information obtained from eHRSS.

3.5.2. eHR healthcare professionals should be aware that each access to HCR's eHR will be logged and monitored.

3.5.3. eHR healthcare professionals should ensure prior and express consent is obtained from the HCRs before disclosure any information obtained from eHRSS to any third party.

3.6. ENQUIRIES AND ASSISTANCE

3.6.1. Staff designated by Healthcare Providers as contact points may approach eHR Office for assistance via e-mail (xxx) or telephone (xxx).

4. ANNEX

4.1. SDM ARRANAGEMENT FOR EHR SHARING

Persons who have given express and informed consent to join eHRSS would be registered in the eHRSS. HCRs registered must give further separate consent to individual healthcare providers(s), from whom they receive healthcare from, to enable those particular healthcare providers to share their records in the eHRSS. Sharing consent to a healthcare provider could be either an "indefinite" or "one-year" consent.

To enable certain HCRs who are incapable of making an informed decision to share their health data, the eHRSSO stipulates that the following types of person can act as "substitute decision makers" (SDMs) to give consent on behalf of these HCRs:

Persons incapable of consenting	Persons who may act as SDM
(a) A minor (below 16)	1. Parents 2. Guardian 3. Persons appointed by court 4. Immediate Family Members 5. HCP
(b) HCR who is not a minor but being incapable for giving consent	1. Guardian 2. Director of Social Welfare 3. Persons appointed by court 4. Immediate Family Members 5. HCP

4.2. HEALTHCARE PROVIDERS IN EHRSS

Healthcare Provider is a person that provides healthcare at one service location may apply to the Commissioner to be registered as a healthcare provider for the System for the location.

A person provides healthcare at one service location if the person –

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 place;
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 home and engages a healthcare professional
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 home for PWDs and engages a healthcare professional
f. is a specified entity that engages a healthcare professional to perform healthcare at one place; or

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 the provision of healthcare.

4.3. HEALTHCARE PROFESSIONALSREGISTERED IN EHRSS

The following healthcare professionals are allowed for sharing in eHRSS:

1. Registered medical practitioner (Cap 161);
2. Registered nurse or enrolled nurse (Cap 164);
3. Registered midwife (Cap 162);
4. Registered dentist (Cap 156);
5. Registered pharmacist (Cap 138);
6. Registered medical laboratory technologist (Cap 359A);
7. Registered radiographer (Cap 359H);
8. Registered dental hygienist (Cap 156B);
9. Registered chiropractor (Cap 428);
10. Registered occupational therapist (Cap 359B);
11. Registered optometrist (Cap 359F);
12. Registered physiotherapist (Cap 359J); and
13. Registered and listed Chinese medical practitioner (Cap 549).

Sharing by different healthcare professionals at different phrases will be reviewed from time to time and announced by eHR Office.

4.4. POLICIES, GUIDELINES & PROCEDURES AND OTHER RELEVANT INFORMATION RELEASED BY EHR OFFICE FOR PARTICIPATING IN EHRSS

General Policies and Guidelines

(a) Patient Information Notice
(b) Conditions for eHR HCP Registration
(c) Guideline for Using eHR Data for Research and Statistics
(d) eHRSS Privacy Policy Statement
(e) eHRSS Personal Information Collection Statement
(f) Guidelines and Procedures for eHR Healthcare Recipient Registration
(g) Guidelines and Procedures for eHR Healthcare Provider Registration
(h) Guidelines and Procedures for eHR Healthcare Staff Registration
(i) Management of Healthcare Recipient Index
(j) eHR Data Retention Policy
(k) Policy and Guidelines for Handling DAR & DCR in eHRSS
(l) Guidelines and procedures for using Hong Kong Identity Card for eHR
(m) FAQs on eHR Data for Research and Statistics
(n) FAQs on eHRSS

eHR Data Standards

(o) eHR Content Standards Guidebook.
(p) Editorial Guide on Hong Kong Clinical Terminology Table – Overview.
(q) Guide on Implementation & Maintenance of the Hong Kong Clinical Terminology Table.
(r) eHRSS Data Requirement Specification

eHR Security and System Connection Guidelines

(s) IT Security Policies for eHRSS
(t) Security Assessment Checklist for Participating in the eHR Programme
(u) eHR Connection Mode Guide
(v) eHRSS Data Interoperability Standards
(w) Communication Protocol (Data Interface) Specification
(x) ELSA Installation Guide
(y) Token Inventory Management User Guide
(z) eHR Adaptor Interface Specification
(aa) Process Report and Exceptional Reporting Requirement

4.5. REFERENCE FROM THE OFFICE OF THE PRIVACY COMMISSIONER FOR PERSONAL DATA (PCPD)

Office of the Privacy Commissioner for Personal Data
(http://www.pcpd.org.hk/)
Personal Data (Privacy) Ordinance (Cap 486)
(http://www.pcpd.org.hk/english/ordinance/ordfull.html)
Data Protection Principles
(http://www.pcpd.org.hk/english/ordinance/ordglance.html)
Code of Practice
(http://www.pcpd.org.hk/english/ordinance/codes.html)
Guideline and Explanatory Booklet
(http://www.pcpd.org.hk/english/publications/code_pra_ex.html)
Guidance Note & Fact Sheet
(http://www.pcpd.org.hk/english/publications/guid_note.html)
Information Book
(http://www.pcpd.org.hk/english/publications/infor_book.html)
Guidance on Data Breach Handling and the Giving of Breach Notifications
(http://www.pcpd.org.hk/english/publications/files/DataBreachHandling_e.pdf)

The references listed out in this COP are by no means exhaustive. The Office of the Privacy Commissioner for Personal Data may issue more Code of Practice or Guideline Note or other material or update any existing documents from time to time. Readers of this COP are advised to access to the internet website of the Office of the Privacy Commissioner for Personal Data for the most updated information (http://www.pcpd.org.hk/).

Annex C

Draft Framework for Handling of Complaints relating to operation of the Electronic Health Record Sharing System (eHRSS)

(Note: This document is a preliminary draft. It serves merely as an indication of the content of the eventual mechanism for handling complaints relating to eHRSS operation.)

Overall principles *(issues to be covered)*

- Fair (e.g. accord priority in accordance with the substance of the complaint, the date of receipt, the adverse consequences of delay, etc.; The subject of a complaint should not handle the complaint himself/herself)
- Consistent (e.g. sufficient guidance and training for officers to handle complaints with consistent approach and procedures)
- Open and Transparent (e.g. keep complainant informed of progress and outcome)
- Facilitative (e.g. effective and well-publicized channels for lodging complaints; written communication with complainant should be in plain language and, as far as possible, in the same language in which the complaint was lodged)
- Respect confidentiality (e.g. as a general rule, information about complaints received and the personal data of the complainants should only be released on a need-to-know basis; where sharing of personal data with other parties is necessary, consent from the complainant (data subject) should be obtained before doing so in order to comply with the Personal Data (Privacy) Ordinance (PDPO, Cap. 486))

Channels for lodging complaints e.g.

- In person
- By phone
- By post
- By email
- By fax

Information to be provided by complainant

- Personal particulars of complainant
- Contact details of complainant
- Identity of party complained against
- Case particulars
- Supporting documents, if any

Initial processing and screening

- Issue written acknowledgement of receipt
- Assign a case number and subject officer to handle complaint
- Record information provided by complainant and seek clarification / further information from the complainant as appropriate
- Examine information provided by complainant and gather information/advice from relevant parties including the party complained against to determine whether a prima facie case can be established (without disclosing the identity / personal data of the complainant)
- Refer cases not within the ambit of eHR Commissioner (eHRC) to other suitable parties for follow-up where appropriate e.g.
  - Complaints relating to any suspected breaches of PDPO regarding the use of personal data in an eHR: referral to the Office of the Privacy Commissioner for Personal Data
  - Complaints relating to corruption and bribery etc.: referral to the Independent Commission Against Corruption
  - Complaints relating to suspected criminal offences under the eHRSS Ordinance: referral to suitable law enforcement agent (e.g. the Police)
- For complaints that should be referred, seek consent of the complainant before making the referral
- For complaints with no prima facie case, inform complainant of reason(s) and his/her options (e.g. ask for a review, lodge an appeal)

Further processing (for established prima facie cases not referred to other parties)

- Look into cases in accordance with relevant policies and guidelines having regard to nature of complaint and gather relevant facts from subject teams regarding the complaint e.g.
  - Complaints relating to the technical matters of eHRSS (e.g.

system malfunctioning, inaccuracy of shared data): IT team; eHRSS Data Interoperability Standards, eHRSS Data Requirement Specification, etc.
    - Complaints relating to attitude / performance of staff: relevant established guidelines for the civil service e.g. on conduct and discipline
    - Complaints relating to refusal / suspension / cancellation of the registration of a healthcare recipient (HCR) / a (registered) healthcare provider (HCP)): registration team
- Obtain further information from complainant as necessary
- Take appropriate actions against complained party e.g.
    - request remedial action
    - verbal warning
    - written warning
    - suspension of registration with eHRSS (only applicable to complaints against HCPs / HCRs)
    - cancellation of registration with eHRSS (only applicable to complaints against HCPs / HCRs)
- Notify complainant of outcome and possible options e.g. ask for review / lodge appeal (for verbal complaints, verbal replies may generally suffice but a written reply should be provided if so requested by the complainant)

<u>Reviews/appeals</u>

- A complainant may ask for a review of how his/her complaint was handled, or may lodge an appeal against the outcome. Where possible, such requests should be considered by an officer senior to the subject officer.
- For decisions of eHRC to refuse / suspend / cancel the registration of an HCR / a (registered) HCP, an aggrieved person may also appeal to the Administrative Appeals Board.

<u>Respective roles of officers</u>

- Subject officers handling complaint: at a minimum rank of Senior Executive Officer or equivalent
- Ultimate authority on major sanctions on HCRs / HCPs (e.g. suspension or cancellation of registration): eHRC

Overall processing time

- Whilst the eHRSS has not commenced operation and therefore we have no operational experience to make reference to, we envisage that:
  - For general cases, written acknowledgement of receipt of a written complaint should be issued within 10 calendar days and a substantive reply within 30 calendar days
  - For complicated cases, longer processing time will be required and the complainant should be kept informed of progress and the reasons why a longer time is needed

Progress monitoring

- All complaints, written or verbal, should be recorded in a central complaints register. It should contain sufficient details of each complaint for progress monitoring and future review as necessary.
- Subject officers should be responsible for updating progress. They should be mindful of long outstanding cases and keep track of follow-up action.

Anonymous complaints

- Depending on the gravity of the allegations made and the adequacy of information for meaningful follow-up, certain anonymous complaints should be treated in the same way as signed complaints though it is not possible to reply to the complainants.

Illustrative flowchart showing major steps