醫健通
ehealth
香港特別行政區政府 HKSAR GOVT

# The Legal, Privacy and Security Framework for Electronic Health Record Sharing Public Consultation Document

eHealth Record Continuity of Care for You

Food and Health Bureau
Hong Kong Special Administrative Region Government

# eHealth Record
# Continuity of Care for You

## The Legal, Privacy and Security Framework for Electronic Health Record Sharing
## Public Consultation Document

Food and Health Bureau
Hong Kong Special Administrative Region Government
December 2011

# Table of Contents

# Message from Dr York Y N CHOW, GBS, JP, Secretary for Food and Health

Dear Citizens,

In 2008, the Government embarked on a reform of our healthcare system to ensure its sustainable development and respond to the increasing healthcare needs of the community. The proposal to develop a territory-wide patient-oriented eHealth Record (eHR) Sharing System was first put forward as one of the service reform proposals and received broad support from the community.

The eHR Sharing System will provide an essential infrastructure for access and sharing of participating patients' health data by authorised healthcare providers in both the public and private healthcare sectors. Through timely sharing, different healthcare providers can provide collaborative patient-centred care more efficiently and in a seamless manner, and to realise the concept of "records follow patients".

The benefits of the system are obvious and participation is entirely voluntary. We would also ensure the privacy and data security of patients in the development of the eHR Sharing System. To this end, we endeavour not only to deploy the appropriate technologies to safeguard system security, but also to formulate specific legislation to provide robust legal protection for the privacy and confidentiality of patient information. Specifically, participating healthcare providers have to be properly authorised and need to follow certain requirements to be set out in the legislation, code of practice or guidelines, in line with the "patient-under-care" and "need -to-know" principles.

We need your participation and your views to realise the potential and benefits of the eHR Sharing System. We are launching this consultation to seek your views on the proposed legal, privacy and security framework for the eHR Sharing System. I encourage you to go through our proposals and share your views and suggestions with us.

Dr York Y N CHOW
Secretary for Food and Health
December 2011

# *Executive Summary*

## The eHR Programme

The Electronic Health Record (eHR) Sharing System is proposed as a key infrastructure for Hong Kong's healthcare system to enhance the quality and efficiency of healthcare provided to our population. It was proposed as one of the healthcare reform proposals put forward in the Healthcare Reform Consultation Document "Your Health, Your Life" published in March 2008.

2. With broad public support received during the healthcare reform consultation in 2008, the Food and Health Bureau (FHB) has put in place the Government-led eHR Programme since 2009, supported by a dedicated eHR Office set up in FHB, to steer and oversee the coherent development of the eHR Sharing System in Hong Kong in both the public and private sectors.

- ***What is eHR sharing?*** An eHR is a record in electronic format containing health-related data of an individual. With an individual's consent, healthcare providers may access the individual's health-related data for his/her healthcare purposes. An eHR Sharing System provides an efficient platform for healthcare providers to upload and access individuals' health-related data.

- ***Why eHR sharing?*** An eHR Sharing System provides an important healthcare infrastructure for healthcare providers to access a patient's essential health-related data for continuous and quality healthcare, allowing seamless interfacing between different healthcare providers, (e.g. doctors and hospitals), enabling more timely treatment and diagnosis, and reducing duplicative diagnostic tests and data gathering.

- ***How is eHR sharing implemented?*** The Government put in place the eHR Programme in 2009 to develop a **patient-oriented** eHR Sharing System for **voluntary participation**, leveraging on the Hospital Authority (HA)'s systems and know-how, through a **building block approach** supported by pilots, and based on open, pre-defined and common standards and protocols.

3. The first stage of the eHR Programme aims to set up the eHR sharing platform by 2013-14 for connection with all public and private hospitals, and have electronic medical/patient record (eMR/ePR)[1] systems available in the private market for private doctors, clinics and other healthcare providers to connect to the eHR sharing platform.

## Objectives of eHR Sharing

4. The objectives of the eHR Sharing System are as follows -

(a) **Improve Efficiency and Quality of Care:** by providing healthcare providers with timely access to comprehensive medical information of patients, and enhancing cost-efficiency by minimising duplicate investigations.

(b) **Improve Continuity and Integration of Care:** by providing healthcare providers with access to lifelong health records of patients for holistic care and facilitating referral and follow-up of cases between different levels of care.

(c) **Enhance Disease Surveillance:** by allowing prompt provision of data for disease surveillance and by facilitating the compilation of health statistics to support policy formulation and public health research.

(d) **Redress Public-Private Imbalance:** by facilitating other public-private partnership in healthcare and at individual level, by enabling patients to choose freely between public and private services without worrying about the transfer of medical records.

[1] eMR/ePR systems are information systems deployed by individual healthcare providers for storing their patients' medical records for their own healthcare purposes. Such systems do not automatically or necessarily provide sharing capabilities. Sharing of eHR by such systems will require compliance with set standards and protocols for sharing and connection to a sharing platform based on such standards and protocol for interconnecting other eMR/ePR systems similarly equipped.

## Need for Framework for Privacy and Security

5. In implementing the eHR Programme, we accord paramount importance to data privacy and system security. We plan to formulate a framework for the eHR Sharing System to give legal protection to data privacy and system security prior to commissioning of the System. This is necessary to instil public confidence in the eHR Sharing System, while giving effect to the objectives of eHR sharing. Currently the Personal Data (Privacy) Ordinance (Cap.486) (PDPO) sets out the general safeguards for personal data privacy applicable across all sectors. We recognise that the nature of patients' health data and their sharing by healthcare providers would require specific and/or additional safeguards on privacy and security. We consider that a legislation specific for governing eHR sharing is needed to complement and supplement the PDPO and to lay down the rules clearly for the operation of the eHR Sharing System.

6. To this end, we have formulated the legislative principles and the Legal, Privacy and Security Framework for eHR sharing (the Framework), having regard to the provisions of PDPO, current clinical practices and professional codes of conduct, and overseas experience of legislation on health information (e.g. Australia, Canada and the United Kingdom), in consultation with relevant stakeholders in the private and public sectors, including representatives of the Office of the Privacy Commissioner for Personal Data (PCPD), the Consumer Council, various healthcare professional groups, patient groups, information technology professionals, HA and the Department of Health (DH). This document sets out our proposals of the Framework for further consulting the public and stakeholders.

## Key Concepts and Principles

7. The key concepts and principles on data privacy and system security for the eHR Sharing System are as follows -

- **Voluntary participation** ("compelling but not compulsory"): only **patients** who choose to participate on **express and informed consent** will have their health data shared through the eHR Sharing System; only **healthcare providers** who **participate and comply** with the requirements for eHR sharing can **upload and access data** through the eHR Sharing System.

- **"Patient-under-care" and "need-to-know":** healthcare providers may access the health data of **only patients for whom they are delivering care and with their consent**, and **only those health data that are necessary for the delivery of care** for the patients; access to eHR Sharing System by healthcare providers will be regulated by legislation to ensure compliance.

- **Pre-defined scope of eHR sharing:** only health data falling within the pre-defined scope for eHR sharing **("eHR sharable scope")** of those patients who have given their consent will be accessible by other healthcare providers over the eHR Sharing System; data that fall outside the eHR sharable scope will **not** be shared through the System.

- **Identification and authentication of patient:** patients will be identified by a **centralised Person Master Index (PMI)** to ensure that health data accessed by healthcare providers through the eHR Sharing System are associated correctly with the individual concerned, and the System will authenticate patients properly for their giving consent or authorisation; data will be "frozen" from access for patients who revoke their consent.

- **Identification and authentication of healthcare providers and professionals:** providers will be identified and authenticated through certifying their eMR/ePR systems or other means. Professionals will also be identified and authenticated by a centralised database to ensure that all health data of patients they upload are attributed correctly to the concerned patients, and all their activities through the eHR Sharing System, including access and changes to data, are logged properly; professionals' access to health data will be subject to role-based access control according to the role of the professionals.

- **Government-led governance and enforcement:** the Government will take the lead in **governing the operation of the eHR Sharing System** and **enforcing the necessary safeguards** to uphold the protection of the data privacy of patients and system security as a paramount priority, while achieving the objectives of eHR sharing for quality healthcare.

- **Privacy of patients and needs of healthcare providers:** the eHR Sharing System should strike a reasonable balance between the protection of patients' **data privacy** and the **clinical needs** of healthcare providers to access and share patients' health data for delivery of healthcare, while maintaining the professional standard of healthcare.

- **Versatile and technology neutral:** the legislative framework for protection of data privacy and system security of the eHR Sharing System should be sufficiently versatile and technology neutral to cater for future advancement in health information technology; a Code of Practice (COP) will be put in place to regulate the operation of the eHR Sharing System.

## Legal Framework for Privacy and Security

8. Based on the key concepts and principles above, and taking into account views from stakeholders, we have formulated the detailed proposals for the Framework as set out in this document, a summary of which is provided in the ensuing paragraphs.

### *Basic Model of eHR Sharing*

9. Participation by patients in the eHR Sharing System will be **strictly voluntary**. Sharing of eHR data will be guided by clinical needs of healthcare providers. This, together with the "patient-under-care" and "need-to-know" principles and regulated access by healthcare providers and other controls over use of eHR, can be summarised in the following simplified basic model of eHR sharing under the Framework.

"***Provider B*** may access, through the **eHR Sharing System**, a piece of **health data** of ***Patient P*** entered by ***Provider A*** **only if** all the following conditions are met -

(1) ***Patient P*** has **participated** in the eHR Sharing System by **express and informed consent**.

(2) Both ***Provider A*** and ***Provider B*** have **participated** in the eHR Sharing System and are subject to **regulated access** to the System.

(3) The piece of health data of ***Patient P*** falls **within the scope of eHR data sharable** through the eHR Sharing System.

(4) ***Provider A*** has the **consent** of ***Patient P*** (see patient's consent below) so as to upload his/her health data to the eHR Sharing System.

(5) ***Provider B*** has the **consent** of ***Patient P*** (including referral) so as to access his/her health data available on the eHR Sharing System.

(6) ***Provider B*** **needs access** to and will use the piece of health data of ***Patient P*** **for delivery of professional healthcare** to ***Patient P***.

(7) All the parties are **uniquely identified and authenticated** and all the above events/activities are **logged** in the eHR Sharing System.

(8) **System security measures** are in place to ensure that access of the health data takes place only if the above are met."

10. The Framework is formulated primarily through refinement of this simplified basic model by considering practical situations for access to and use of eHR Sharing System. Deviations and exceptions are proposed only where justified having regard to circumstances or current practices. Individual aspects of the above model are elaborated in the following sections.

### *Patient's Consent*

11. Patients' participation must be based on **express and informed consent**. In practice, to assist patients to make an informed decision, information on the scope, purpose and use of eHR, the rights of patients, privacy and security safeguards, and withdrawal arrangements will be provided. Certain specific proposals are made to facilitate the giving of consent by patients for access by providers -

(a) A patient can give consent to a healthcare provider for access/uploading to his/her eHR in two forms: (i) a time-limited one-year rolling consent that will lapse after one year from the date when the healthcare provider last provided care to the patient; (ii) an open-ended consent that will continue to remain valid until expressly revoked by the patient.

(b) Special arrangements will be made for consent to be given on behalf of patients, minors below the age of 16, and mentally incapacitated persons (MIPs) by substitute decision makers (SDMs), in circumstances where they are considered incapable of giving informed consent on their own.

(c) If a patient chooses to participate in eHR sharing, he/she will be required part and parcel of registration to give open-ended consent for HA and DH as health-care providers to access/upload to their eHR, given that HA and DH hold health records essential for healthcare.

(d) The eHR Sharing System will provide features to facilitate referral of a patient between healthcare providers in line with current referral practices; specifically, if a patient is referred by Provider A to Provider B for healthcare, Provider A may specify the part of eHR where Provider B will have access to.

(e) Access to the eHR of a patient without his/her prior consent will be allowed under exceptional circumstances such as emergency; such access must be in compliance with the PDPO and will be subject to stringent control over who and in what circumstances may have such access.

12. A patient may withdraw from eHR sharing and revoke his/her consent at any time. For legal and audit purposes, arrangements will be put in place to "freeze" the data from access but retain the data in an archive for a specified period (see retention of eHR data below). A patient who chooses to re-join eHR sharing within the frozen period will have his/her eHR data re-activated, but he/she would need to revalidate all consents previously granted to individual healthcare providers. A patient who chooses to re-join eHR sharing after the frozen period will no longer have his/her previous eHR data available and will have his/her eHR compiled afresh as with any new participant in eHR sharing.

### *Defined Scope of eHR Sharing*

13. We formulated the proposed scope of data for eHR sharing (eHR sharable scope) taking into account the clinical need of healthcare professionals to provide healthcare to patients. We also proposed to introduce the scope of sharable eHR data by phases, both to tie in with the technical capability of the eHR Sharing System, and also to be in tandem with the use of the eHR Sharing System by healthcare providers.

14. The proposed scope of eHR sharable data is set out in detail at **Annex D** of this consultation document. It will cover the following components in the first phase of development of eHR sharing -

(a) personal identification and demographic data
(b) episodes/encounters with providers (summary)
(c) referral between providers
(d) adverse reactions/allergies
(e) diagnosis, procedures and medication
(f) immunisation records
(g) laboratory and radiology results
(h) other investigation results

15. For completeness and integrity of the eHR to ensure professional standards of healthcare provided to patients, in principle healthcare providers will, subject to the "patient-under-care" and "need-to-know" principles and consent given by patients, be allowed access to any health data within the eHR sharable scope uploaded by other health-care providers. Unless otherwise prescribed through access control under the eHR Sharing System in line with the stated principles, the eHR Sharing System will not provide for any particular health data falling within the eHR sharable scope to be concealed from access or be subject to additional consent. Participating healthcare providers will be required to make available health data in their eMR/ePRs falling within the eHR sharable scope for uploading to the eHR Sharing System with no exclusion.

### *Access to, Use and Retention of eHR Data*

16. The primary use of eHR sharable data is for the continuity of care of patients. Healthcare providers participating in eHR sharing will be required to observe the relevant rules regulating the use of data available through the eHR Sharing System. Access to and use of eHR data by healthcare providers in any other circumstances are not allowed in principle, and will be subject to audit on compliance. The general exemptions under the PDPO on access to and use of personal data may apply depending on the circumstances, but such application will be subject to control by the eHR Sharing System operating body (eHR-OB) to ensure compliance.

17. As a specific exemption, for the potential benefit of public health, data in the eHR Sharing System may be used for disease surveillance and public health research, subject to a mechanism to be prescribed under the future eHR legislation as a secondary use. Specifically, the use of non patient-identifiable eHR data for disease surveillance and public health research will be approved by the eHR-OB. However, the use of patient-identifiable data for diseases surveillance and public health research will be subject to prior approval by the Secretary for Food and Health on the recommendation of a research board.

18. As a general rule, eHR data of patients will be kept within the eHR Sharing System for as long as they continue to participate in eHR sharing. For patients who withdraw from eHR sharing, or who passed away, their data on the eHR Sharing System will be "frozen", i.e. archived and debarred from access by any healthcare providers. With reference to various legal provisions and professional practice, such data will continue to be kept for three years for patients who withdraw and ten years for deceased patients. After the frozen period, the eHR would be de-identified[2] and retained in the system for secondary use such as disease surveillance and public health as mentioned above.

### *Identification, Authentication, Access Control and Security*

19. To ensure correct attribution of eHR data to patients and authentication of providers for eHR data upload and access, a series of security measures will be put in place and enshrined in the proposed COP and Operating Guidelines for eHR sharing (see below), including -

(a) **Identification and authentication of patients:** through primarily the use of Hong Kong Identity Card (HKID, or Smart ID Card) with system data validation (e.g. checking of HKID check digit); use of other supplementary means of identification and authentication will be devised for patients without HKID; a PMI will be centrally maintained by the eHR Sharing System to uniquely identify and attribute eHR data to individual patients.

(b) **Identification and authentication of providers:** healthcare providers accessing the eHR Sharing System would be identified and authenticated through certifying their eMR/ePR systems or other means; integrity and origin of the health data would be established by the eHR Sharing System through centralised certification, and all uploading, accessing and changing of health data on the eHR Sharing System by individual healthcare providers would be logged to ensure that all data and activities could be properly ascribed to the originating professionals.

[2] To de-identify is to make it impossible to identify the eHR data with any patients.

(c) **Role-based access control by healthcare professionals:** all eMR/ePR systems connecting to the eHR Sharing System would be required to implement a role-based access control, i.e. healthcare professionals with different roles would be granted different levels of access to content and functions (e.g. only doctor can upload prescription but not nurses) in the eMR/ePR systems and in turn data uploaded to and accessed on the eHR Sharing System; further check on health-care professionals' access against a central healthcare professional registry will be performed by the eHR Sharing System; logs on access made through the eMR/ePR systems would be maintained and subject to audit and inspection.

(d) **System-wide security measures:** high-security encryption will be applied to all relevant data in the databases, files and archives in the eHR Sharing System, as well as to all data during transmission between the eHR Sharing System and individual eMR/ePR systems; downloading of eHR data from eHR Sharing System will be restricted to PMI data and allergy information to minimise risk; system alerts will be provided to a patient through electronic means (e.g. Short Message Service or emails) on eHR Sharing System activities related to him/her (e.g. when his/her eHR is accessed); individual eMR/ePR systems will also be required to adopt security measures and follow COP and operating guidelines to ensure security at the user end.

### *Data Access and Correction by Patients*

20. In line with the provisions of the PDPO, patients as data subjects may request for data access at a fee to be prescribed. However, we propose that the future eHR legislation should apply a more stringent standard than the current PDPO over data access request, in that the request must be made by the subject patients themselves or their SDMs (such as parents of minors or guardians of MIPs) but not any other third parties even if authorised by the patients. This is to ensure a higher standard of data privacy and to ensure that only the patient himself, apart from his healthcare providers to whom he has given consent, could gain direct access to his health data, as opposed to any other third parties on his behalf.

21. Under the eHR Sharing System, healthcare providers who contribute the health data of a patient can make amendment to the patient's health data on their own initiatives or at the request of the patient in line with existing clinical practices. In line with PDPO, a patient can also request correction on his/her eHR data, and such data correction request under the eHR Sharing System will be handled by the healthcare provider from whom the data originated. The provider may correct the data, or refuse to do so if it does not agree that the data is inaccurate, in which case it should make a note of the matter. As mentioned above, all such changes or remarks will be logged by the eHR Sharing System as part of the system-wide security measures, and any amendment will be appended to the eHR instead of replacing the original data. Changes or remarks made will also be highlighted for healthcare providers who subsequently access the eHR to facilitate their reading of the eHR. To prevent circumvention of security safeguards, editing of PMI data of a patient would require the subject patient's consent.

### *COP, Guidelines, Security Audits, Complaints and Reviews*

22. Under the Framework, we propose to formulate a set of COP on rules and regulations regarding participating healthcare providers' internal access procedures and control, as well as security standards and requirements for eMR/ePR systems. The COP is proposed to be issued by the eHR-OB and binding on healthcare providers in that their eMR/ePR systems are required to comply with the COP. Non-compliance with the COP per se does not lead direct to legal liability under the eHR legislation. However, they should be backed by specific authority under the eHR legislation, such that where breach of data privacy or system security is found in case of review of complaints and security checks or audits, the eHR-OB may require remedial actions to be taken by users and managers of individual eMR/ePR systems in compliance with the COP.

23. We also propose that the eHR-OB may publish non-statutory operating guidelines, best practices, procedural standards and/or other form of guidelines concerning how individual eMR/ePR systems should operate and behave, and how interconnection with and access to eHR Sharing System should be made. While these guidelines are not mandatory by legislation, they may be taken into account when the eHR-OB certifies an eMR/ePR system for compliance with the required security standards and fit for interconnection with the eHR Sharing System, or when it

grants a healthcare provider or its healthcare professionals access to the eHR Sharing System. This will help maintain high data privacy and system security standards without having to impose inflexible rules that cannot be adapted in the light of changes in technology.

24. To ensure compliance and as a check and balance, the eHR-OB should be empowered to perform security audits on the eMR/ePR systems and the internal access control of healthcare providers. Such checks or audits may be performed at random pick or on account of complaint. Regular security audits would also be conducted on the eHR Sharing System and its interconnection with individual eMR/ePR systems to ensure its safe and secure operation. Apart from security audits, the technical design of the eHR Sharing System would also build in a number of protection features against security breaches through continuous system monitoring to detect any identifiable irregular patterns such as frequent access to large number of patient records, and extensive amendments (see below).

25. A mechanism to initiate review and resolve complaints relating to eHR sharing will be devised under the future eHR legislation. This is to allow complaints to be made and reviews to be initiated on data privacy and system security matters relating to the access to and use of eHR data, the eHR Sharing System itself, or individual eMR/ePR systems connected to the Sharing System.

### *Criminal Sanctions*

26. To create deterrent effect against breach of data privacy and system security of the eHR Sharing System, we propose to introduce a new criminal sanction specifically against unauthorised access to the eHR Sharing System with a malicious intent. The level of criminal sanctions will be set with reference to existing sanctions against similar actions under other provisions[3]. We do not intend to create criminal liabilities against innocent errors in inputting eHR data or other unintentional contraventions by healthcare professionals in their delivery of healthcare to patients in good faith.

[3] Section 27A of the Telecommunications Ordinance (Cap.106) (a fine of $20,000 on conviction) and Section 161 of the Crimes Ordinance (Cap.200) (imprisonment for 5 years upon indictment).

## Technical Aspects of Data Privacy and System Security

27. To ensure a coordinated approach on both the legal and technical fronts, the legal and security safeguards have to be considered in tandem with the current eHealth technologies and application in Hong Kong as well as the technical design and operation of the future IT infrastructure for the eHR Sharing System.

### *Security and Technical Design of eHR Sharing System*

28. Due to its sensitive nature and the need to reside in the Internet environment, we attach great importance to the security infrastructure for eHR. After careful consideration, we propose to adopt a central data repository approach instead of other approaches (e.g. distributed storage of eHR Sharable Data). A consultancy study was commissioned to validate our proposal and concluded that it was in the right direction and had covered relevant technical aspects. One of the principles adopted by HA in the architectural design of the eHR core sharing infrastructure (eHR Core) is "building security in" to protect data security and patient privacy.

### *Security and Audit Framework*

29. In addition to the infrastructural tools such as authentication and authorisation, firewalls and intrusion detection tools, a comprehensive security and audit framework should be established. Such framework should cover all areas including policies, standards, system design, certification, issues management as well as training and communication. Specifically, it would include the establishment of a set of security policy and protocols for the eHR Core and eMR/ePR systems (e.g. eMR/ePR systems are required to install specific security software); definition of security processes for software development and threat management; and recommendations for security risk assessment, with reference to local and overseas experiences. A consultancy study on the IT security and audit framework was commissioned in late 2010 to ensure that these security aspects are properly reviewed and addressed.

### *Privacy Impact Assessment and Privacy Compliance Audit*

30. To ensure the compliance of the eHR Sharing System with the privacy protection standard, we will conduct a privacy impact assessment (PIA)[4] and privacy compliance audit[5] in accordance with the guidelines issued by PCPD to ensure that the privacy protection concepts are implemented effectively. To this end, we first commissioned a PIA scoping study to review the Framework as well as to formulate the overall PIA strategy plan.

31. The PIA scoping study concluded that the Framework is in compliance with the local regulatory requirements and comparable with overseas practices, and recommended some refinement and clarification. We accordingly further refined the Framework in the light of the findings of the consultancy study.

[4] A PIA is generally regarded as a systematic risk assessment tool that can be usefully integrated into a decision-making process. It is a systematic process that evaluates a proposal in terms of its impact upon personal data privacy with the objective of avoiding or minimising adverse impacts.

[5] The privacy compliance audit aims at (i) assessing and evaluating the level of privacy compliance with the PDPO, in particular the six Data Protection Principles in Schedule 1 to PDPO, with respect to the collection, processing and handling of personal data; (ii) identifying potential weaknesses in the data protection system; and (iii) providing recommendations for a review of the data protection system.

## Way Forward

32. We are consulting the public on the Framework and welcome your views which would be instrumental to the success of the eHR Sharing System. Please send your views on this consultation document to us on or before **11 February 2012** through the contact below.


Address: Electronic Health Record Office
Food and Health Bureau
19/F, East Wing, Central Government Offices
2 Tim Mei Avenue, Tamar, Hong Kong

Fax: (852) 2102 2570

e-mail: eHR@fhb.gov.hk

Website: www.ehealth.gov.hk


33. In parallel, we are working on the design and development of the IT infrastructure and would factor in the findings of the consultancy study on the IT security and audit framework commenced last year. We will, based on the PIA strategy plan, proceed with a full PIA study, the first phase of which would focus on the existing pilots, namely the revamped Public-Private Interface – Electronic Patient Record project after integration with other pilots such as the eHealth System for elderly vouchers. The PIA would examine the implementation of some of the data and privacy protection concepts as proposed above. Taking into account the results of the public consultation, we would refine the Framework and incorporate the amendment in the scope of the PIA study as appropriate and prepare for drafting the eHR legislation.

# *Chapter 1: Introduction*

## Background

### *Electronic Health Record (eHR) Sharing as an Essential Infrastructure for Healthcare Reform*

1.1 An eHR is a record in electronic format containing health-related data of an individual. With the consent of the individual, the data can be uploaded and accessed by different healthcare providers for healthcare-related purposes. The proposal to develop a territory-wide patient-oriented eHR Sharing System was put forward as one of the proposals in the Healthcare Reform Consultation Document "Your Health, Your Life" published in March 2008, and received broad support from the community among other service reform proposals.

### *Objectives*

1.2 The eHR Sharing System is an essential infrastructure for implementing the healthcare reform. The objectives of developing the Sharing System are as follows –

(a) **Improve Efficiency and Quality of Care:** by providing healthcare providers with timely access to comprehensive medical information of patients, and enhancing cost-efficiency by minimising duplicate investigations and treatments.

(b) **Improve Continuity and Integration of Care:** by providing healthcare providers with access to lifelong health records of patients for holistic care and facilitating referral and follow-up of cases between different levels of care.

(c) **Enhance Disease Surveillance:** by allowing prompt provision of data for disease surveillance and by facilitating the compilation of health statistics to support policy formulation and public health research.

(d) **Redress Public-Private Imbalance:** by enabling patients to choose freely between public and private services without worrying about the transfer of medical records, and facilitating other public-private partnership in healthcare.

### *Benefits of eHR Sharing*

1.3 The eHR Sharing System brings the following benefits –

(a) For clinicians, eHR will improve availability and transparency of information shared, allowing seamless interfacing between healthcare providers in both the public and private sectors. Healthcare providers will be able to access the right information at the right time. This will allow healthcare providers to improve the efficiency of their healthcare interventions and reduce the number of consultations that are necessary for achieving the desired outcome. Associated efficiency gains will be realised in avoiding the need to store, collate and transfer paper records. Record transportation costs will also be avoided.

(b) For patients, eHR will enhance the quality of care by –

(i) reduction in the frequency and scale of medication errors;
(ii) more efficient and effective use of diagnostic tests;
(iii) timely treatment, for example, by eliminating repeated tests or information requests from a patient; and
(iv) improved accuracy of diagnosis and disease management through clinical decision support.

(c) For the healthcare system as a whole, the eHR Sharing System minimises duplicate tests and errors associated with paper records, and enables more efficient and better quality healthcare. The eHR Sharing System also enables disease surveillance and compilation of health statistics for public health and policy making.

## Developing a Territory-wide Patient-oriented eHR Sharing System

### *The Steering Committee on eHR Sharing*

1.4 To take forward the development of the eHR Sharing System, the Secretary for Food and Health (SFH) established the Steering Committee on eHR Sharing (Steering Committee) in July 2007. The Steering Committee, supported by working groups, provides advice to the Food and Health Bureau (FHB) on the formulation of strategies to facilitate the development of eHR infrastructure and the sharing of patients' eHR in both the public and private sectors. The membership list of the Steering Committee is at **Annex A**.

### *Key Guiding Principles in eHR Development*

1.5 The territory-wide patient-oriented eHR Sharing System is developed along five key guiding principles –

(a) eHR development should be government-led and should leverage the Hospital Authority (HA)'s systems and know-how;

(b) the eHR Sharing System should be based on open, pre-defined and common technical standards and operational protocols;

(c) development of the eHR Sharing System should be based on a building block approach, involving partnership with the private sector;

(d) participation in eHR sharing should be compelling but not compulsory for both patients and healthcare providers; and

(e) data privacy and system security of the eHR Sharing System should be accorded paramount importance and given legal protection.

### *The eHR Programme*

1.6 The full development of the eHR Sharing System straddles over 10 years from 2009-10 to 2018-19. In July 2009, the Finance Committee of the Legislative Council (LegCo) approved a new commitment of $702 million for the first stage of the eHR Programme (from 2009-10 to 2013-14). A dedicated eHR Office was set up in the FHB to steer and oversee the eHR Programme to ensure coherent development in both the public and private sectors. The Government will leverage the successful experience and invaluable expertise of the HA in its development of the Clinical Management System (CMS) since 1995. The HA CMS is the largest integrated electronic medical/patient record (eMR/ePR) system in Hong Kong and has more than nine million medical records. The Government will make available HA's systems and know-how to facilitate the private sector to develop their eMR/ePR systems with sharing capabilities through different partnership initiatives such as the eHR Engagement Initiative (EEI).

### *Targets of First Stage eHR Programme*

1.7 For the First Stage eHR Programme, we aim to –

(a) set up the eHR sharing platform by 2013/14 for connection with all public and private hospitals;

(b) have eMR/ePR systems and other health information systems available in the market for private doctors, clinics and other health service providers to connect to the eHR sharing platform; and

(c) prepare an eHR-specific legislation for the eHR Sharing System to protect data privacy and system security prior to commissioning of the system.

1.8 The eHR Office, under the guidance of the Steering Committee, will spearhead and co-ordinate the eHR Programme which covers –

(a) development of the eHR Core Sharing Infrastructure (eHR Core) for the territory-wide eHR sharing platform;

(b) development of the CMS Adaptation Modules and On-ramp Applications for the private sector to adopt and deploy;

(c) standardisation of technical standards to facilitate accurate sharing of clinical data;

(d) different partnership initiatives including EEI to invite partnership proposals that would contribute to the development of the eHR Sharing System;

(e) various engagement and briefing sessions with stakeholders and public consultation to raise public interest in and awareness of eHR;

(f) formulation of an eHR specific legislation to safeguard data privacy and ensure the integrity of the eHR Sharing System; and

(g) Privacy Impact Assessment (PIA), Privacy Compliance Audit, Security Risk Assessment[6] and Security Audit[7] to ensure that the eHR Sharing System complies with the relevant legislation and requirements.

We would report further on the progress and detailed proposals on the formulation of an eHR specific legislation later in this Document.

---

[6] Security Risk Assessment can be defined as a process of evaluating security risks, which are related to the use of information technology. It can be used as a baseline for showing the amount of change since the last assessment, and how much more changes are required in order to meet the security requirements.

[7] Security Audit is a process or event with the security policy or standards as a basis to determine the overall state of the existing protection and to verify whether the existing protection has been performed properly. It targets at finding out whether the current environment is securely protected in accordance with the defined security policy.

# *Chapter 2: Progress to Date*

2.1 Since 2009, we have made good progress in implementing the eHR Programme in various fronts. Pilot projects are carried out and the technical infrastructures are beginning to take shape. We are also engaging stakeholders in various partnership projects and promoting the concept of eHR sharing through various publicity efforts. We have also mapped out a framework to protect data privacy and system security for eHR sharing.

## eHR Sharing Pilot

### *Public-Private Interface – Electronic Patient Record (PPI-ePR) Sharing Pilot Project*

2.2 To test the feasibility and acceptability of eHR sharing, we have launched the PPI-ePR pilot project through HA since April 2006, allowing participating private health care providers and other registered institutions to view their patients' medical records kept at HA, subject to the patients' consent. By end September 2011, the PPI-ePR pilot has enrolled over 170,000 patients, 2,470 private healthcare professionals, 13 private hospitals and 58 other private or non-governmental organisations (NGOs) providing services related to healthcare (including their 348 residential care homes or centres), and received very positive feedback from both participating patients and healthcare providers.

2.3 The Government will continue to expand this one-way eHR sharing pilot to more private healthcare professionals and NGOs to allow more patients and private healthcare providers to experience the sharing of patients' records electronically. The security and privacy protection measures deployed in this pilot, including a two-factor authentication

of each participating healthcare professional[8], proper authorisation by patients[9], as well as notification to patients[10], have been found to be satisfactory by both external and internal audits. We integrated the sign-on mechanism of the eHealth System (eHS)[11] with that of PPI-ePR in July 2010, allowing healthcare professionals to use the same token for logon to both PPI-ePR and eHS. PPI-ePR would become part of eHR before the eHR Sharing System comes into operation in 2013-14, to facilitate the development of full fledged eHR sharing.

### *Radiological Image Sharing Pilot Project*

2.4 The Radiological Image Sharing Pilot was launched in January 2009. It allows participating private healthcare providers with patient's consent to send radiological images of enrolled patients to HA via electronic means. By end September 2011, four private hospitals and two private radiology centres have already participated in the programme. The pilot will be expanded to other interested private healthcare providers.

### *Cataract Surgeries Programme*

2.5 This pilot public-private partnership (PPP) scheme was launched in February 2008. Eligible patients are subsidised to undergo cataract surgeries in the private sector. Participating private healthcare providers are allowed to upload clinical information of their patients and view the patients' medical records kept at HA through the PPI-ePR platform, hence making two-way eHR sharing possible. By end September 2011, 99 private doctors have participated in this programme and about 12,000 patients have received surgeries.

---

[8] The participating healthcare professionals are given a two-factor authentication, the first being their log-in ID and password, the second in the form of a security token.

[9] The patient enrolled in the pilot will be provided with his/her own access key. He/she will be required to produce the password to the participating healthcare professional to allow the latter's access to the patient's record.

[10] A message via short message service will be sent to the patient whenever his/her record is being accessed.

[11] eHS is a web-based system which serves as an electronic platform on which voucher-based and subsidy schemes operate. The eHS captures key particulars of patients for administering targeted subsidisation for private primary healthcare services.

### *Tin Shui Wai Primary Care Partnership Project*

2.6 The programme has been implemented by HA in Tin Shui Wai North since June 2008 and Tin Shui Wai South since June 2010. The programme allows chronic disease patients in stable conditions and in need of long-term follow-up treatment at public general out-patient clinics (GOPCs) to receive treatment from private doctors with partial subsidy provided by the Government. It aims at testing the use of PPP model and supplementing the provision of public general out-patient services in the area. Under the programme, participating private doctors can upload their patients' clinical information and view the patients' clinical records kept at HA through the PPI-ePR platform. The system helps build up a continuous record for chronic disease patients receiving follow-up treatment at public GOPCs. By end September 2011, over 1,600 patients and 10 private doctors participated in the programme.

### *Haemodialysis Public-private Partnership Programme*

2.7 A three-year pilot project was launched in March 2010 under which patients with end-stage renal disease receiving follow-up treatment at HA are given a subsidy to receive haemodialysis services in community haemodialysis centres operated by the private sector or NGOs. A specially designed electronic information system was developed to allow sharing of clinical information between HA and the community haemodialysis service providers. By end September 2011, a total of 87 patients and five community haemodialysis service providers participated in the programme.

### *Patient Empowerment Programme*

2.8 Starting from March 2010, a pilot patient empowerment programme has been implemented in selected clusters of HA in collaboration with NGOs to improve chronic disease patients' knowledge of their diseases and to enhance their self-management skills. A multi-disciplinary team comprising allied health professionals from HA develops appropriate teaching materials and aids for common chronic diseases and provides training for frontline staff of the participating NGOs. An electronic information system was developed to allow sharing of patients' clinical information between HA and the

participating NGOs. By end September 2011, there were a total of 15,543 patients participating in the programme and the programme is extended to all seven clusters of HA.

### *Public-Private Chronic Disease Management Shared Care Programme*

2.9 The programme has been implemented in Sha Tin and Tai Po in the New Territories East Cluster of HA since March 2010, and in Wan Chai and Eastern District in the Hong Kong East Cluster since September 2010. Under the programme, participating chronic disease patients can choose participating private doctors as the main healthcare providers to follow up on their conditions according to the care frameworks, while the public system will continue to provide support services for chronic disease patients and private doctors. It aims at testing the feasibility and effectiveness of a PPP model for enhancing the provision of continuous and comprehensive care and support for chronic disease patients based on the care frameworks for diabetes mellitus and hypertension developed by the Working Group on Primary Care[12]. An electronic platform has been developed for timely, two-way sharing of clinical information between HA and the participating private doctors. By end September 2011, a total of 239 patients and 60 private doctors participated in the programme.

2.10 These pilots have provided a proof-of-concept on the feasibility and acceptability of eHR sharing amongst healthcare providers and patients in general. They have also provided valuable experience and insights into the potential challenges of implementing eHR Sharing System on a territory-wide and population-wide basis. The pilots and their future evolution will form essential building blocks for the eHR sharing infrastructure.

[12] The Working Group on Primary Care is set up under the Health and Medical Development Advisory Committee chaired by the SFH to provide strategic recommendations on enhancing and developing primary care in Hong Kong.

## Technical Development

### *eHR Core*

2.11 The eHR Core is developed to prepare for the designing and building of the eHR sharing platform for interconnecting individual eMR/ePR systems adopted by individual healthcare providers. The blueprint for the eHR Core has been formulated. The eHR Core will support a standard-based, robust and secure central platform for sharing patients' eHR. The system will be based on common standards to be developed by the public and private sectors in collaboration.

2.12 The eHR Core architecture is based on a centralised eHR sharable data store, following the five principles below –

- *Building-block Approach:* Follow a building-block approach to mitigate the risks of evolving user requirements and expedite realisation of benefits through deployment of small blocks of functionalities.

- *Service Oriented Architecture*[13]*(SOA):* Adopt an SOA to ensure reusability and extensibility of each developed module.

- *Building Security in:* Design the system by "building security in" to protect data security and patient privacy.

- *Built-in Sustainability:* Built-in sustainability of the clinical data beyond people and system life-span to ensure longitudinal access of individual patients' health records.

- *High Level System Serviceability:* Construct for a high level of system serviceability to ensure capability to support the 7 days x 24 hours (7x24) healthcare environment.

[13] SOA is a design paradigm in application development. In SOA, individual functions of an application are modularised and presented as services for client applications. These services are loosely coupled in nature. Applications can be built by composing one or more services without having to know their underlying implementation.

2.13 We will establish a central data store of the eHR sharable data. All incoming data by participating healthcare providers to the central eHR data store will be transformed, restructured, standardised and re-formatted before storage to the eHR Sharing System.

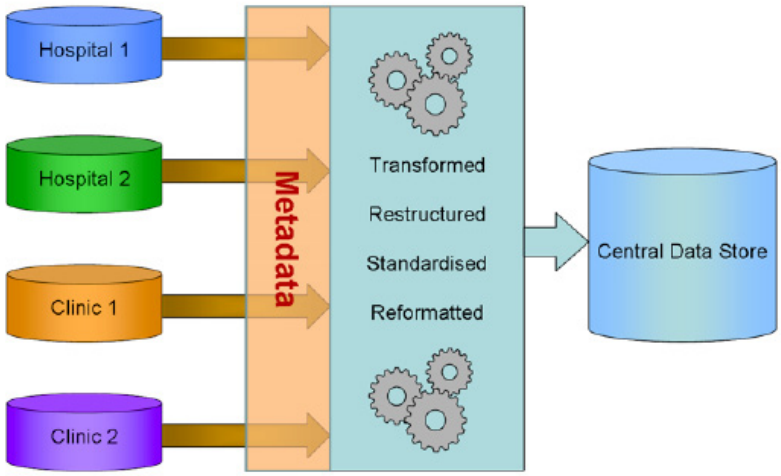


*Figure 1 – Central Data Store for eHR*

## *Clinical Management System (CMS) Adaptation and CMS On-ramp*

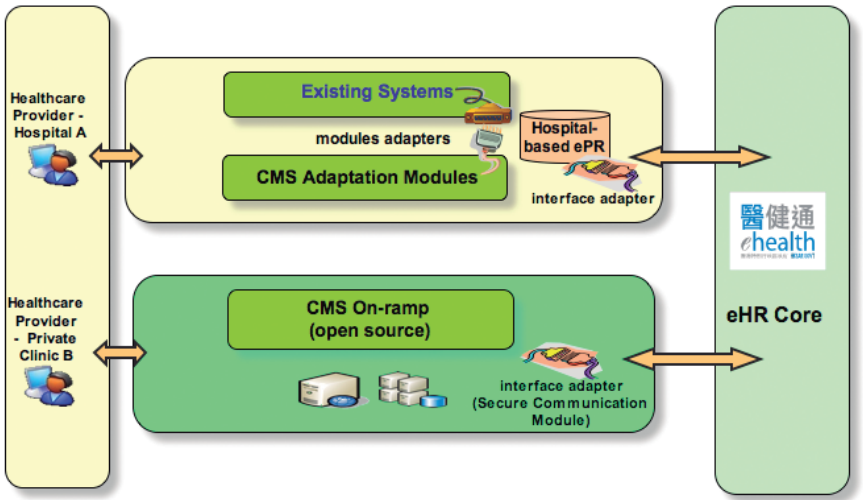


*Figure 2 – CMS Adaptation and CMS On-ramp*

2.14 The blueprint for the CMS extension components has also been formulated. The CMS extension components facilitate the adoption and deployment of CMS by private healthcare providers, especially private hospitals and clinics which would like to adopt CMS components for their own use with minimal investment and maintenance.

2.15 There are two key elements for the CMS extension components, namely CMS Adaptation and CMS On-ramp. Firstly, leveraging on HA CMS, CMS Adaptation modules will be developed to enable data sharing and integration capabilities by private hospitals or institutions. The CMS Adaptation modules may include Person Master Index (PMI) services; structured allergy and alert input; medication order entry; diagnosis and procedure; outpatient consultation summary; discharge summary; letter engine for generating certificates and documents (e.g. medical and attendance certificates); drug allergy checking services; hospital-based ePR, etc. The modules will be developed and released using a building-block approach. Private hospitals or institutions can adopt the modules by integrating them into their own eMR/ePR systems.

2.16 Secondly, CMS On-ramp is an open source and open standard clinic management system with the ability to share the clinical data of patients with the eHR Sharing System. It will be made available to provide low investment cost access for private solo or group practice healthcare providers to the eHR Sharing System.

2.17 These extension components will be implemented predominantly through private participation. For instance, license may be granted to private healthcare providers and/or information technology (IT) vendors for their use of adapted and extended components and technologies of HA's CMS. The strategy of the development, sourcing and hosting of the CMS Adaptation modules for private hospitals and CMS On-ramp applications for private practitioners has also been formulated. These modules and applications will be provided to the private healthcare sector for free or at minimal cost. The cost of implementation and hosting of the CMS Adaptation and CMS On-ramp will be borne by private healthcare providers.

### *eHR Standardisation and Interface*

2.18 Standard terminology is the foundation for the development of an interoperable eHR. The objectives of standardisation and interfacing component are as follows –

- to reduce cost of technical integration by allowing systems to interoperate and interconnect in a uniform way through the eHR sharing infrastructure and relieve system developers from building separate interfaces;
- to avoid errors by reducing miscommunication;
- to advance a compliance verification platform for testing interoperability that could support a future compliance scheme for individual eMR/ePR systems of healthcare or IT service providers;
- to provide technical support for private healthcare providers which already have their own eMR/ePR systems and would like to connect to eHR; and
- to provide the necessary interface to facilitate such interconnection.

2.19 The initial set of eHR standards were published on the eHR Office website[14] for healthcare providers' and IT vendors' reference. The standards will be further refined based on recommendations from stakeholders.

[14] The initial eHR standards include the eHR Content Standards Guidebook and the Data Interoperability Standards. The eHR Content Standards Guidebook lays down the principles to build the eHR and defines the data standards for identifying a person, a provider, encounters and other health data. The Data Interoperability Standards set out the message standards for sending health data to the eHR Sharing System. The standards were published on http://www.ehealth.gov.hk.

2.20 A position paper on Terminology Management for eHR sharing was published on the eHR Office website[15] in August 2010. The paper identifies current issues in terminology management in Hong Kong, recommends the standard terminologies for building an interoperable eHR and sets out the approach for the establishment of a Hong Kong Clinical Terminology Table (HKCTT) to support the development of interoperable eHR Sharing System.

2.21 The HKCTT, based on HA's Clinical Vocabulary Table, will be built by 2012. The following international terminologies will be integrated into HKCTT –

(a) Systematised Nomenclature of Medicine, Clinical Terms (SNOMED CT);

(b) International Classification of Diseases, 10th Revision (ICD-10);

(c) Logical Observation Identifiers Names and Codes (LOINC); and

(d) International Classification of Primary Care 2 (ICPC2)

2.22 A drug table mapped to SNOMED CT will also be built. The drug table will incorporate the existing Compendium of Registered Pharmaceutical Products which includes all registered drugs in Hong Kong. Health Level 7 (HL7) will be used as the messaging standard for eHR sharing in Hong Kong. HL7 Hong Kong Ltd.[16], a private company, was set up for the local development and adoption of HL7.

[15] http://www.ehealth.gov.hk/en/information_standards/information_standards_documents.html

[16] HL7 is a globally adopted message standard in healthcare. It is one of several American National Standards Institute-accredited Standards Developing Organisations operating in the healthcare arena. In September 2009, the HL7 Plenary accepted the application of Hong Kong joining the HL7 as an affiliate member. This allows the setting up of the HL7 Hong Kong Ltd. for developing and adapting HL7 standards to meet local requirements.

## EEI and Partnership Projects with Professional Bodies

### *EEI*

2.23 The eHR Office launched the first and second stages EEI exercise to invite private healthcare and IT stakeholders to submit partnership proposals contributing to the development of a territory-wide eHR Sharing System in October 2009 and November 2010 respectively. More than 50 EEI proposals from private healthcare stakeholders were received in the first stage, and implementation of on-going engagement plans for the partnership proposals commenced in mid-2010. The EEI proponents were invited to join user groups and task force meetings to discuss user requirements, and to participate in different pilot projects for testing the concept of eHR sharing.

2.24 With reference to the partnership projects and development needs raised by private healthcare stakeholders during the first stage, the second stage EEI was launched in November 2010 to invite innovative proposals contributing to the development of the eHR Sharing System from the IT professional bodies and private IT vendors. 58 EEI proposals were received and the engagement plans were formulated.

### *Partnership Projects with Healthcare Professional Bodies*

2.25 To facilitate the participation of private healthcare providers in eHR sharing, sponsorship was provided to the Hong Kong Medical Association (HKMA) to upgrade their open source clinic management system (HKMA CMS 3.0) for private doctors, develop an integration hub for connection to the eHealth Voucher and Vaccination Subsidy schemes as well as to provide streamlined capability for reporting of notifiable diseases to Central Notification Office of the Centre for Health Protection, and to provide training for doctors. By end September 2011, about 520 doctors have installed the HKMA CMS 3.0.

2.26 We sponsored the Hong Kong Dental Association in developing a first-of-its-kind open source clinic management system for dentists in Hong Kong. We also provided funding support to the Hong Kong Association of Medical Laboratories to develop a laboratory integration platform for laboratory information exchange, and provide training and technical support for the private laboratory practitioners. The entire solution will be an open source system and made available free of charge to the laboratory sector and clinics in Hong Kong. All these partnership projects with professional bodies not only promote IT application in the healthcare sector, but also pave the way for the participation of healthcare providers in eHR sharing.

## Promotion and Publicity

2.27 To promote eHR sharing, we are making use of various channels, including the eHR Office website and video broadcast in various public hospitals and clinics, to explain the concept of eHR sharing and its benefits. We conducted briefing sessions to patient groups, professional bodies, academic institutions and NGOs and collaborated with healthcare professional bodies in training IT and healthcare professionals in eHealth applications and health informatics. We will continue to explore other ways to promote the benefits of eHR sharing. With this multi-pronged approach, we hope to enhance the public's understanding of eHR sharing and instil a patient-oriented culture of sharing patients' records for the purpose of better healthcare.

## Legal, Privacy and Security Framework

2.28 Given the importance of data privacy in the eHR Programme, we have also mapped out the proposed legal, privacy and security framework (the Framework) for the eHR Programme. The approach to the formulation and details of the Framework are set out in Chapters 3 and 4.

# *Chapter 3: Approach to the Formulation of the Legal, Privacy and Security Framework*

3.1 Privacy and data security are of paramount importance to the development of a territory-wide eHR Sharing System. Public confidence in the System and their voluntary participation have to be underpinned by stringent protection of eHR data. This requires not only appropriate technologies to safeguard data security and minimise the risk of leakage of personal health data, but also rigorous procedures and policies for the use of eHR data, and continuous effort in providing education and training to all stakeholders to enhance their privacy awareness.

## Engagement of Stakeholders

3.2 We fully appreciate the public concern over data privacy and security, and the need to tap the major participants' views on the eHR Sharing System at an early stage, so that the Framework will meet the expectation of the industry and the public. The Working Group on Legal, Privacy and Security Issues (WG) was therefore formed with the responsibility to examine legal and related issues relating to the eHR sharing infrastructure and to formulate recommendations on the legal aspect of the Framework as well as interim solutions to address these issues. The membership list of the WG is at **Annex B**. Through the WG, we have engaged stakeholders including healthcare professional bodies, private hospitals, IT experts, patient groups, the Office of the Privacy Commissioner for Personal Data (PCPD), the Consumer Council, HA and the Department of Health (DH) to gauge their views and concerns. The wide membership of the WG is to ensure that the eHR Sharing System would not only provide the necessary legal, privacy and security safeguards, but also cater for the practical need of an efficient and sustainable information system, as well as the clinical workflow for the delivery of quality care to the patients.

# Chapter 3: Approach to the Formulation of the Framework

## Approach to the Formulation of the Framework

3.3 The WG first looked at the different stages of data management life cycle and considered the issues on data collection, usage, disclosure, access and correction, and retention. In deliberating the issues to be covered under the Framework, in particular the legal issues, we have made reference to –

(a) the existing legal provisions and guiding principles governing personal data privacy under the Personal Data (Privacy) Ordinance (Cap.486) (PDPO) as well as other relevant legislation;

(b) the existing code of practice for healthcare professionals;

(c) overseas legislation on health information, particularly in jurisdictions where an eHR sharing system is also under development, such as Canada, Australia, and the United Kingdom; and

(d) the current clinical practice.

3.4 The WG also examined some of the intended functionalities of the eHR Sharing System as well as the viability of different safeguard measures to ensure that the Framework would not pose technical and operational problems to the eHR Sharing System. The participation of IT professionals and members with experience in eHS and eMR/ePR systems has greatly benefited the discussion. Through this partnership, we strive to balance privacy protection and data security with practicality and efficiency of information flow, in order to enhance public confidence in the eHR Sharing System.

## Principles for Safeguarding eHR Information

3.5 In formulating the Framework, we have carefully considered the PDPO, the Data Protection Principles (DPPs) in Schedule 1 under PDPO (at **Annex C**), as well as the well-established principles governing doctor-patient relationship and clinical practices. The very constructive advice and active participation of PCPD are invaluable. The issues considered under these principles are set out below -

(a) *Principle 1 - purpose and manner of collection of personal data*

In line with DPP1, we need to work out the model and mechanism to obtain the express and informed consent of patients in eHR sharing. The proposed consent model covers the nature, duration of validity of patients' consent, and special consent arrangement for patients who may not be capable of making an informed decision, for example those in an emergency situation or mentally incapacitated persons (MIPs). It is generally agreed that the elderly, minors or MIPs are the categories of patients who would stand to benefit most from the eHR Sharing System, particularly in the delivery of healthcare through data on drug allergy or discharge summary for follow-up treatment. We therefore aim at a mechanism that would facilitate the granting of consent with due regard to protecting their privacy. In accordance with DPP1, we also need to define the scope of data to be collected and decide on whether patients can have discretion on the scope of data to be covered in their eHR.

(b) *Principle 2 - accuracy and duration of retention of personal data*

The usefulness of eHR as clinical reference for treatment and healthcare purposes hinges on the accuracy and quality of the data collected. First and foremost, we have to ensure the correct attribution of the records to the patients. This requires proper authentication of the patient and the healthcare providers. In this respect, we have to look for a possible unique identifier in the PMI (a set of demographic and personal data for identification purposes) of the eHR and the means to verify it. Furthermore, standardisation of data and information standards facilitates reliable and proper data management. We would need to work out suitable measures to ensure data quality and the integrity and origin of data. A

system allowing correction or amendment to eHR data, either at the patients' or the healthcare providers' initiative, would also need to be established.

We realise that as an electronic platform, the eHR Sharing System cannot verify the accuracy, completeness or truthfulness of the eHR data uploaded. We should make clear that the healthcare provider who contributes the data should ensure the data accuracy. One important requirement under DPP2 is that personal data shall not be kept longer than is necessary for the fulfilment of the purposes of its collection. In that regard, we have to differentiate between the "active" eHR of participating patients, and the eHR of withdrawn or deceased patients. A reasonable retention period and a suitable mechanism to store the latter are necessary.

(c) *Principle 3 - use of personal data*

The Government has made it clear that the primary purpose of the eHR Sharing System is for the continuity of care of patients, and better integration and collaboration of different healthcare providers in the delivery of care. Apart from that, it is widely recognised that an efficient health information system should allow meaningful and beneficial secondary uses, for example, in disease surveillance and public health research. One of our tasks is therefore to deliberate a mechanism under the Framework to enable such secondary uses for person-identifiable data as well as non person-identifiable data for the wider public interest, with due regard to the privacy of patients.

(d) *Principle 4 - security of personal data*

Privacy and security protection go in tandem. To accord adequate security, policy measures under the Framework as well as technical security tools built in under the IT infrastructure are required. Since the eHR Sharing System would be accessible by different participating healthcare providers, checking against unauthorised access and authentication of healthcare providers would form the first line of defence. Given the multi-disciplinary team care in some healthcare settings, apart from the authentication of the eMR/ePR systems of the healthcare providers at the system level, we also need to ensure that access by authorised

healthcare professionals is in line with the principle of "patient-under-care" and on a "need-to-know" basis. Differentiated role-based access control as another level of defence and authentication against professional registration of the healthcare workers are options to be examined.

On the technical level, data encryption, access logging, notification of access, access bar, restriction against downloading of data and other automatic safeguards need to be developed. While the Framework should be technology neutral, the inter-relation between privacy and security measures should be well co-ordinated for system operability and an efficient clinical workflow.

(e) *Principle 5 - information to be generally available*

To ensure patients' understanding of the eHR Sharing System and to enhance transparency, we have to work out the scope of information that needs to be brought to the attention of patients upon their joining and the appropriate means to inform them. Also, appropriate access alert and notification to patients in different circumstances should be built in.

(f) *Principle 6 - access to personal data*

Following the requirements under s.18 to s.25 and DPP6 of the PDPO on an individual's general right of access to and correction of his/her personal data, the Framework would need to set out the access rights and the detailed mechanism to meet the data access request of the patients as well as procedures to effect a correction by patients under the eHR.

3.6 In addition to issues covered by the DPPs, we need to study the current clinical practices, such as the referral arrangement and the different roles and functions played by laboratories and the allied health sector under a team-care environment, so that the information flow under the eHR Sharing System would enhance the efficiency and integration of different healthcare providers. In particular, we need to consider the following long-established principles.

(a) *Patient-under-care*

There is a trust relationship between patients and healthcare professionals. This trust relationship underlines not only medical treatment but also the safekeeping of the patients' records. This relationship not only entitles the relevant healthcare professionals to access patients' records, but also obliges them to keep the information safe in the best interest of the patients. These duties are set out in some professional codes of practice. We have to align the Framework with these codes of practice.

(b) *Need-to-know*

Under the principle of "patient-under-care", healthcare professionals are required to observe that patients' records would only be accessed or disclosed on a "need-to-know" basis. This necessitates the differentiated role-based access by different healthcare professionals under a team-care setting. This principle would also need to be duly reflected in the sharing of a patient's eHR under a referral arrangement.

## Need for a Specific Legislation

3.7 While PDPO sets out the general safeguards for personal data privacy, given the sensitivity of health data, the speed at which such data may be disseminated in an electronic environment, and the amount of data to be shared on the eHR Sharing System, we consider that an eHR legislation is necessary to provide for specific and/or additional privacy and security safeguards for the eHR Sharing System to instil public confidence in the System.

3.8 In considering the above issues, we also made reference to the experience and mechanism in other jurisdictions and have taken note of the difference between the electronic environment in which the eHR Sharing System operates and the functionalities of its technical infrastructure for processing and storing the data, and the current paper-based system or an eMR/ePR system without sharing capability.

## Review of the Framework – PIA

3.9 The proposed Framework was mapped out along the approach above, incorporating the views of stakeholders. As with other major IT systems and to ensure the compliance of the eHR Sharing System with privacy protection standards, we will conduct a PIA and a privacy compliance audit in accordance with the guidelines issued by PCPD to ensure the effective implementation of privacy protection requirements. After WG's deliberation on the Framework, we commissioned a PIA scoping study to review the Framework as well as to formulate the strategy plan for the full scale PIA.

3.10 The PIA scoping study concluded that the Framework is, generally speaking, in compliance with the local regulatory requirements and comparable with overseas practices, with some issues that required further clarification and refinement. With the concerted effort and advice from PCPD, the Department of Justice and other relevant parties, and in the light of the findings of the PIA scoping study, we further refined the Framework. We would implement the recommended strategy plan in commissioning the full scale PIA.

## Technical Aspects of Data Privacy and System Security

3.11 To ensure a co-ordinated approach on both the legal and technical fronts, we have ensured that the legal and security safeguards have to be considered in tandem with the current eHealth technologies and application in Hong Kong as well as the technical design and operation of the future IT infrastructure for the eHR Sharing System.

### *Security and Technical Design of the eHR Sharing System*

3.12 HA, as the technical agency for the eHR Sharing System, is responsible for the design and development of the eHR Core. One of the principles in the architectural design of the eHR Core is to design the System by "building security in" to protect data security and patients' privacy.

3.13 Due to the sensitive nature of health data and the need for the eHR Sharing System to reside in the Internet environment, we attach great importance to the security infrastructure for the eHR Sharing System. After careful consideration, we propose to adopt a central data repository approach instead of other approaches (e.g. distributed storage of eHR Sharable Data). A consultancy study was commissioned to validate our proposal and concluded that it was in the right direction and had covered relevant technical aspects.

### *Security and Audit System*

3.14 In addition to the infrastructural tools such as authentication and authorisation, firewalls and intrusion detection tools, a comprehensive security and audit system should be established. Such system should cover all areas including policies, standards, system design, certification, issues management as well as training and communication. A consultancy study on the IT security and audit framework was commissioned in late 2010 to ensure that these security aspects are properly reviewed and addressed.

3.15 The study was completed in May 2011 and the consultant has made various recommendations including (a) the establishment of a set of security policy and protocols for the eHR Core and eMR/ePR systems that are connected to the eHR Sharing System (e.g. eMR/ePR systems are required to install specific security software); (b) definition of security processes for software development and threat management; (c) recommendation for security risk assessment, protection, monitoring, incident management mechanism, on-going response and assurance activities, with reference to local and overseas experiences; (d) development of a training and communication plan; and (e) the engagement of an independent third-party to perform security review of the system.

## Security Standard and Requirement for Participating Healthcare Providers

3.16 In Hong Kong, most private hospitals have their own eMR/ePR or hospital information systems. That said, these systems vary widely in sophistication and run on different computer hardware and software platforms. IT adoption in the clinical settings has been generally low and most processes for documentation are still manual. Most solo practices are still operating with manual processes while some have computers to capture only the patients' basic demographic information and their insurance schemes. In short, we have to facilitate them to build up the capability to capture electronic clinical information and enable them to share these records in the territory-wide eHR Sharing System.

3.17 Hence, the main targets of the first stage of the eHR Programme are to set up the eHR sharing platform by 2013-14 for connection with all public and private hospitals and to have eMR/ePR systems and other health information systems available in the market for private doctors, clinics and other health service providers to connect to the eHR sharing platform. To achieve this, standardisation of information standards is a key step. Also, to ensure the security of the eHR Sharing System as a whole, we have to work with the private healthcare sector to set the security standards and requirements not only for the eHR Core but also for the participating healthcare providers. These have also been considered by WG in consultation with other relevant working groups. The proposed security and audit framework also lays down the ground rules for the IT sector to design eMR/ePR systems compatible and capable of sharing with the eHR Sharing System.

3.18 To ensure compliance with the security requirement of the eMR/ePR by participating healthcare providers, a proper certification, audit and monitoring mechanism is to be stipulated in the Code of Practice (COP) to be made under the Framework.

3.19 Under the approach outlined above, we have held a lot of discussions with various stakeholders and are happy to say that the Framework has been finalised covering the full data management cycle and the issues outlined above. The details and rationale behind different proposals on the Framework are elaborated in the next Chapter.

# *Chapter 4: The Legal, Privacy and Security Framework*

## Introduction

4.1 In this chapter, we will set out the proposed Framework in detail and the consideration behind. The Framework has been discussed at the WG and endorsed by the Steering Committee. Through the WG, we engaged the relevant stakeholders including healthcare professional bodies, patient groups, and the PCPD. A full list of the WG members is at **Annex B**.

4.2 In the discussion, the WG took into account the existing legal provisions in Hong Kong (particularly those under the PDPO and the recent review of the PDPO), legislation and experience in overseas jurisdictions, the current medical practice and clinical workflow, patients' concerns, the sensitivity of health data and the operability of the eHR Sharing System. This will ensure that the Framework would render adequate protection to data privacy without compromising the efficiency of clinical workflow. The Framework has also been reviewed in the PIA Scoping Study commissioned by the eHR Office in August 2010. The study concluded that the Framework is in compliance with the local regulatory requirements and comparable with overseas practices.

## Need for an eHR-specific Legislation

4.3 Currently PDPO sets out the safeguards for personal data privacy. Since eHR sharing involves the speedy transmission of an enormous amount of sensitive data through the uploading and retrieval of patients' health data by various healthcare providers in the public and private sectors, it is recognised that an eHR-specific legislation is necessary to provide specific and/or additional safeguards (e.g. requirement of express and informed consent of patients for data sharing to a specific doctor) on privacy and security to instil public confidence in the eHR Sharing System. Taking into account the requirements of PDPO, the current clinical practices and the experience overseas, we propose the detailed proposals as set out below.

## Key Concepts and Principles

4.4 Based on the approach set out in Chapter 3, we formulate the following key concepts and principles on data privacy and system security for the eHR Sharing System -

(a) **Voluntary participation:** eHR sharing should be compelling but not compulsory. Only patients who choose to participate on express and informed consent will have their health data shared through the eHR Sharing System. Only healthcare providers who participate and comply with the requirements for eHR sharing can upload and access data through the eHR Sharing System;

(b) **"Patient-under-care" and "need-to-know":** healthcare providers may access the health data of only patients for whom they are delivering care and with their consent, and only those health data that are necessary for the delivery of care for the patients. Access to eHR Sharing System by healthcare providers will be regulated to ensure compliance;

(c) **Pre-defined scope of eHR sharing:** only health data falling within the pre-defined scope for eHR sharing ("eHR sharable scope") of those patients who have given their consent will be accessible; data that fall outside the eHR sharable scope will not be shared through the eHR Sharing System;

(d) **Identification and authentication of patient:** patients will be identified by a centralised PMI to ensure that health data accessed by healthcare providers through the eHR Sharing System are associated correctly with the individual concerned;

(e) **Identification and authentication of healthcare providers and professionals:** providers will be identified and authenticated through certifying their eMR/ePR systems or other means. Professionals will also be identified and authenticated by a centralised database on the basis of various professional registers to differentiate the level of permitted access (role-based access control) to ensure that all health data of patients they upload are attributed correctly to the subject patients, and all their activities through the eHR Sharing System, including access and correction to data, are logged properly;

(f) **Government-led governance and enforcement:** the Government will take the lead in governing the operation of the eHR Sharing System and enforcing the necessary safeguards to uphold the protection of the data privacy of patients and system security as a paramount priority, while achieving the objectives of eHR sharing for quality healthcare;

(g) **Privacy of patients and needs of healthcare providers:** the eHR Sharing System should strike a reasonable balance between the protection of patients' data privacy and the clinical needs of healthcare providers to access and share patients' health data for delivery of healthcare, while maintaining the professional standard of healthcare; and

(h) **Versatile and technology neutral:** the legislative framework for protection of data privacy and system security of the eHR Sharing System should be sufficiently versatile and technology neutral to cater for future advancement in health information technology; a COP will be put in place to regulate the operation of the eHR Sharing System.

## Framework Proposals

4.5 The eHR Programme is territory wide and open to all patients and healthcare providers in Hong Kong. Unlike some of the overseas systems (e.g. Singapore and Estonia where patients are in the system unless they opt-out), participation of patients and healthcare providers in Hong Kong will be **strictly voluntary.**

### *Enrolment of Patients to the eHR Sharing System*

4.6 To enrol in eHR sharing, a patient may complete an enrolment form by visiting any eHR enrolment points located in the premises of HA or DH, private hospitals or premises of other participating healthcare providers, or through other means such as mail or fax to signify to the eHR Sharing System operating body (eHR-OB) his/her express and informed consent to join eHR sharing. Upon successful enrolment, the patient can then grant consent to individual healthcare providers to access/upload data to his/her eHR through the eHR sharing platform. The participation in eHR sharing is illustrated below.

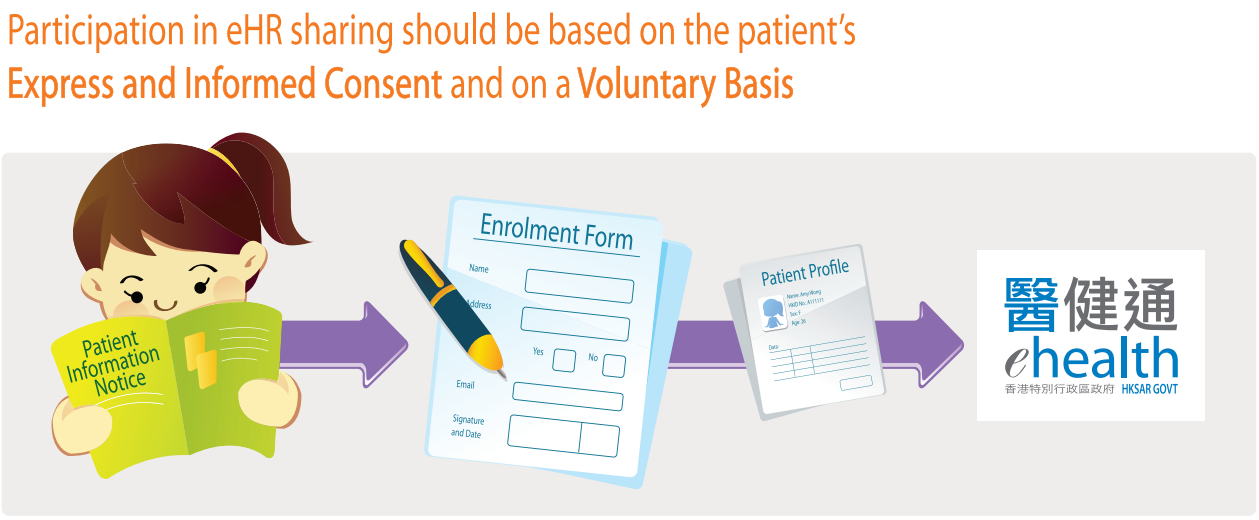


*Figure 3 – Participation in eHR Sharing*

### *Relationship-based Consent Model*

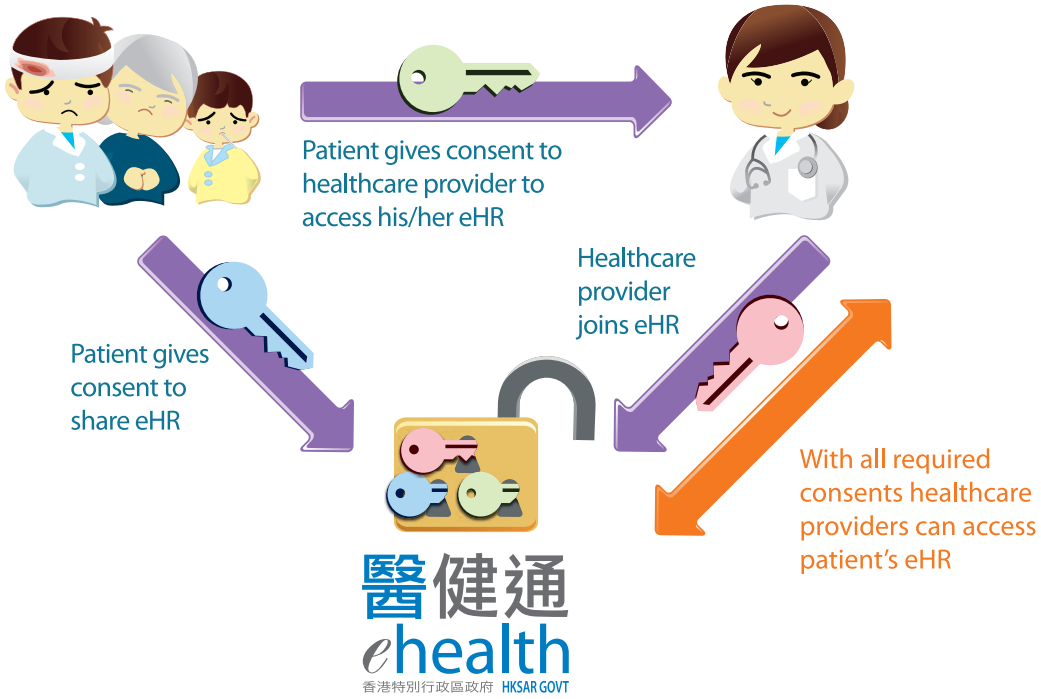


***Figure 4 – Relationship-based Consent Model***

4.7 In line with the long established principles of "patient-under-care" and "need-to-know" in the healthcare profession, the WG proposed and the Steering Committee endorsed a relationship-based consent model, building on the trust between patients and healthcare providers. To participate in eHR sharing –

(a) healthcare providers (such as private clinics, private hospitals) by signing user agreements with eHR-OB shall agree to share all data (including historical data) falling within the eHR sharable scope if readily sharable electronically belonging to the patients who have enrolled in eHR sharing and granted an express and informed consent to the subject healthcare provider. Data that fall outside the eHR sharable scope can be retained in the healthcare provider's eMR/ePR system without sharing to the eHR Sharing System, or in paper records; and

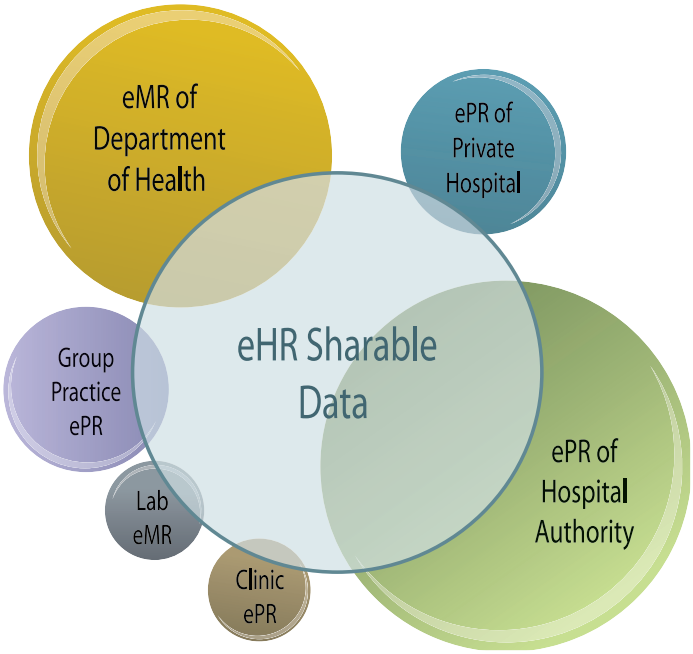


*Figure 5 – eHR Sharable Data*

(b) patients need to give express and informed consent to eHR-OB for enrolling to eHR sharing, which covers the consent to HA and DH for accessing and uploading/ transferring the patients' health data to their eHR (see paragraph 4.14); and to individual participating healthcare providers for their access to the subject patients' eHR, which would also cover the future eHR access or referrals (see paragraph 4.16) by that specific healthcare provider for the treatment purpose of the patients.

## *Patient Information Notice*


***Figure 6 – Patient Information Notice***

4.8 To facilitate the patients' informed decision, we propose that an information notice be handed out to patients upon their enrolment. The information notice may cover details about the scope, purpose, and benefits of eHR sharing; consent to HA and DH; the rights of the patients; the privacy and security safeguards; the referral arrangement; and the withdrawal arrangement. Such information notice should be easy to understand, well publicised through brochures, websites, pamphlets, etc. Multilingual and other special formats (e.g. format for the visually impaired) of the notice will also be provided as appropriate.

## *Conditions for eHR Sharing*

4.9 ***Provider B*** may access, through the **eHR Sharing System**, a piece of **health data** of ***Patient P*** entered by ***Provider A*** **only if** all the following conditions are met -

(a) ***Patient P*** has **participated** in the eHR Sharing System by **express and informed consent.**

(b) Both ***Provider A*** and ***Provider B*** have **participated** in the eHR Sharing System and are subject to **regulated access** to the System.

(c) The piece of health data of ***Patient P*** falls **within the scope of eHR data sharable** through the eHR Sharing System.

(d) ***Provider A*** has the **consent** of ***Patient P*** so as to upload his/her health data to the eHR Sharing System.

(e) ***Provider B*** has the **consent** of ***Patient P*** (including referral) so as to access his/her health data available on the eHR Sharing System.

(f) ***Provider B*** **needs access** to and will use the piece of health data of ***Patient P*** **for delivery of professional healthcare** to ***Patient P***.

(g) All the parties are **uniquely identified and authenticated** and all the above events/activities are **logged i**n the eHR Sharing System.

(h) **System security measures** are in place to ensure that access of the health data takes place only if the above are met.

### *Validity of Consent of Patients*

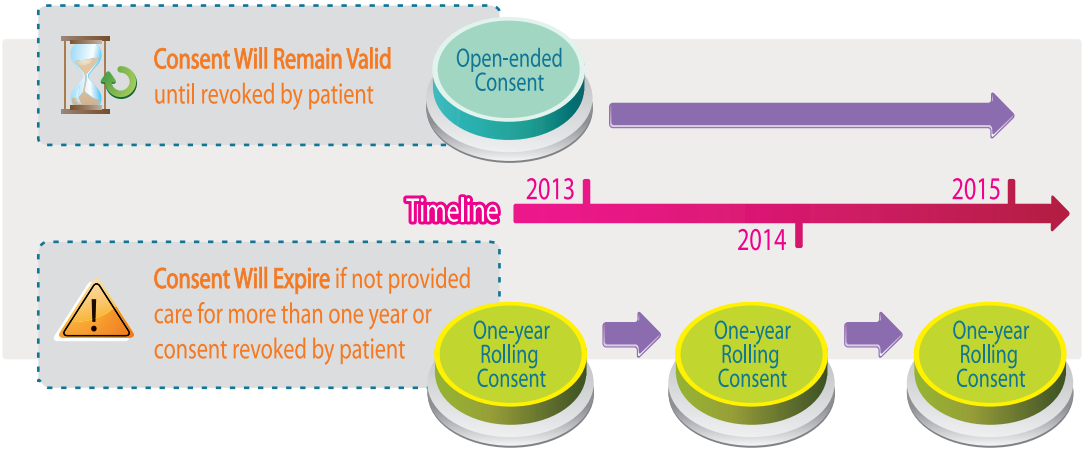


*Figure 7 – Time Limit of Patients' Consent to Healthcare Providers*

4.10 To ensure that only authorised access to eHR would be allowed, to give patients greater control over the access to their eHR, and to cater for patients who may visit a healthcare provider only once but not again, we propose that patients may have two options on the validity of consent to healthcare providers, i.e. a one-year rolling consent or an open-ended consent until revocation. The one-year rolling consent to a healthcare provider counts from the date when the healthcare provider last provided care to the patient, and would expire if that particular healthcare provider had not provided care to the subject patient for more than one year; or when the patient revokes the consent, whichever is earlier. The open-ended consent will remain valid until revocation by the patient.

## *Special Consent Arrangement*

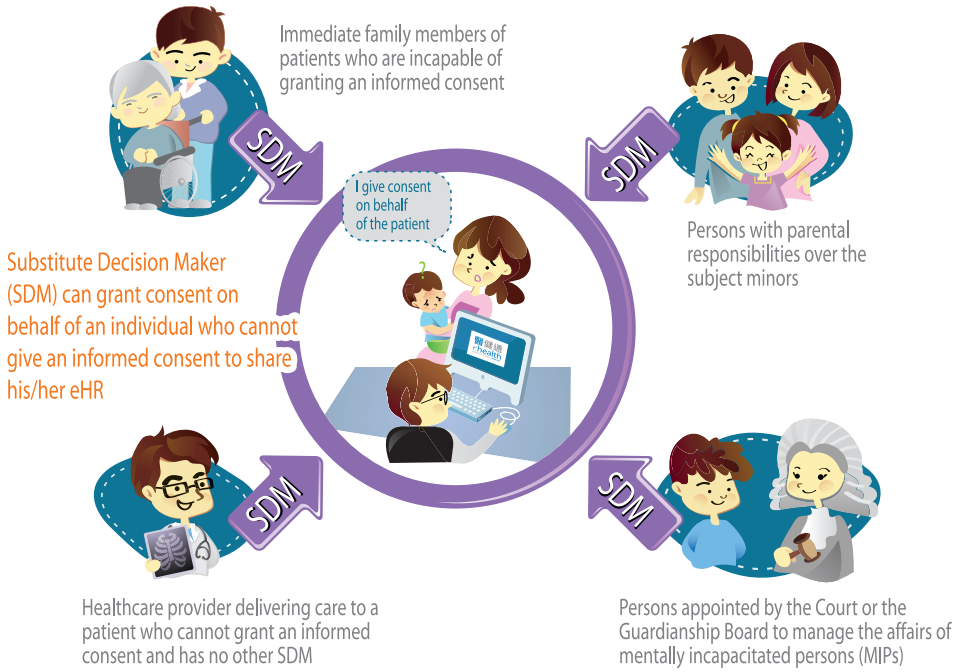


***Figure 8 – Special Consent Arrangement***

4.11 There is currently no specific legal provision for substitute consent on behalf of any individual unable to make an informed decision to share his/her health data. To put it beyond doubt, it is proposed that the eHR legislation would stipulate the right for "substitute decision makers" (SDMs) to grant consent on behalf of these individuals to share their eHR. SDM may include, inter alia, persons with parental responsibilities over the subject minors, persons appointed by the Court or the Guardianship Board under the Mental Health Ordinance (Cap.136) to manage the affairs of MIPs (referred hereafter as "guardians of MIPs"), and other immediate family members[17] of patients. A healthcare

[17] Reference may be made to section 2 of the Family Status Discrimination Ordinance (Cap.527), which provides that "immediate family member", in relation to a person, means a person who is related to the person by blood, marriage, adoption or affinity.

professional may also act as an SDM if it is delivering care in the best interest of a patient who cannot grant an informed consent and has no other SDM. This is to enable health-care providers such as elderly homes to deliver better care to single elderly people under their care. Based on the discussion with stakeholders (including healthcare providers and patient groups), it is considered that the definition of SDM to cover immediate family members or healthcare providers acceptable and would entail limited privacy risk as the consent is only to allow sharing of the subject patients' eHR among healthcare professionals for treatment or care purposes. Healthcare professionals should see to it that the substitute consent aligns with the best interest of the patient in terms of his/her healthcare.

### *Definition of Minors*

4.12 In considering the arrangement regarding SDMs for minors, we have made reference to various local and overseas legislation –

(a) The Interpretation and General Clauses Ordinance (Cap.1) stipulates that a "minor" is a person who has not attained the age of 18.

(b) Section 14(2) of the Parent and Child Ordinance (Cap.429) stipulates that the consent of a minor who has attained the age of 16 years to the taking from himself of a bodily sample shall be as effective as it would be if he were of full age; and where a minor has by virtue of this subsection given an effective consent to the taking of a bodily sample it shall not be necessary to obtain any consent for it from any other person.

(c) Section 8 of the United Kingdom's Family Law Reform Act 1969 stipulates that if a minor over the age of 16 has given an effective consent to any treatment, it shall not be necessary to obtain any consent from his/her parent or guardian.

(d) Section 23 of Ontario's Personal Health Information Protection Act 2004 stipulates that a parent of a minor below the age of 16 may grant consent to the collection, use or disclosure of personal health information.

4.13 We propose that in general[18], individuals at or over the age of 16 should be capable to consent to share their eHR. The age limit is considered appropriate given the maturity of adolescents for giving consent to share their eHR. For a minor under the age of 16, an SDM may grant substitute consent for him/her to participate in order to build a womb-to-tomb eHR. If a minor gives consent in the absence of an SDM, or is in dispute with his/her SDM on sharing of his/her eHR, healthcare providers should exercise their professional judgement to assess whether the minor has the sufficient understanding and intelligence to understand the nature of eHR sharing, with reference to the Gillick test[19]. If the minor is considered capable of consent, his/her view would prevail; otherwise, his/her SDM's view would prevail. This is in line with existing medical practice regarding medical treatment for minors. When a minor attained the age of 16, he/she may make any decision to re-affirm/override any decision previously made by his/her SDM in respect of his/her participation in eHR sharing. The minor may indicate his/her relevant decision, which may cover all substitute consents previously granted to healthcare providers and eHR-OB in one go, on the first consultation at a participating healthcare provider after his/her 16th birthday.

### *HA and DH Records*

4.14 HA and DH offers public healthcare services to every citizen in Hong Kong. Patients' health records at HA and DH will form the essential building blocks of patients' eHR to enhance the continuity of care of the patients. In 2009, around 90% of inpatient service (in terms of bed-days) was provided by HA. HA records relating to patients' hospitalisation form a solid and indispensable part of a patient's eHR for follow up consultation and clinical reference. Also, an infant's record with DH is a valuable basis for a womb-to-tomb health record. To enhance the completeness and integrity of patients' eHR upon their joining of eHR sharing and ensure continuity of care to patients, we thus propose

[18] Except for cases such as adult MIPs, elderly people incapable of giving informed consent, etc.

[19] The Gillick test came from the UK case of Gillick v West Norfolk and Wisbech Area Health Authority [1985] 3 All ER 402 (HL). The test is whether a child has sufficient understanding and intelligence to enable him to understand fully the medical treatment proposed (known as "Gillick" competence). A person who has reached the age of 16 years should be regarded as competent to give consent unless there is evidence to the contrary. The parents' right to determine whether a child under 16 should have medical treatment terminates when the child achieves sufficient intelligence and understanding to make that decision himself.

that patients' consent to HA and DH for accessing and uploading data to their eHR shall be part and parcel of their enrolment to eHR sharing mentioned in paragraph 4.7(b). The eHR legislation would provide for the transfer of the patients' eHR sharable data in HA and DH to the eHR Sharing System. This arrangement saves patients from having to separately register with HA and DH. Once the patients complete their enrolment to eHR sharing, their relevant health data held in HA and DH's eMR/ePR systems would be uploaded to the eHR Sharing System and become sharable by other healthcare providers which have got the patients' consent. This arrangement would be set out clearly in the information notice handed out at enrolment.

### *Referral Arrangement*

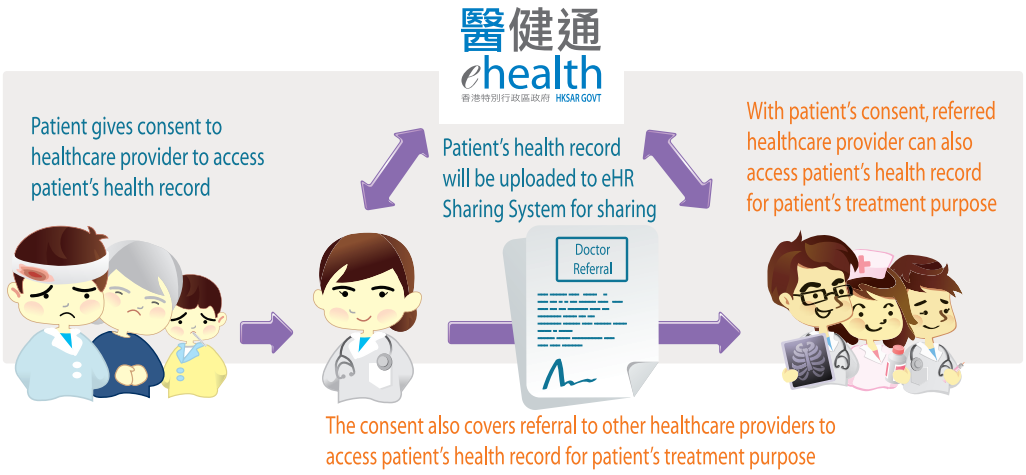


***Figure 9 – Referral Arrangement***

4.15 In line with DPP3 in Schedule 1 of PDPO, personal data in the patient's eHR may be used for a purpose directly related to the original purpose of collection. Under the current medical practice, healthcare providers ("referring provider") would often refer a patient to other healthcare providers such as specialists or laboratories ("referred provider") to facilitate team-oriented healthcare delivery. It is important for the referred providers to be provided with the patient's relevant health information (e.g. results of medical tests) in order to provide proper service to the patient. Normally, the referring provider would attach a medical record or note when making a referral and/or

patients would be asked to bring along their old records/test results for reference. Access to eHR would greatly enhance the quality and effectiveness of care delivered by referred providers. Without a referral arrangement, such access would not be possible unless a patient attends a referred provider such as a laboratory in person and give consent to its access to his/her eHR. This would significantly affect the current clinical workflow especially in cases where physical presence of the patients is not required or not possible.

4.16 We therefore propose that the eHR Sharing System should allow referring providers to specify or attach eHR data that he/she considered relevant to the medical treatment of the patient in the "e-referral" [20] through the eHR Sharing System. The patient information notice would set out this referral arrangement in accordance with DPP1(3). The referred provider can use the attached eHR data to improve the quality of its service. In case further information is required, the referred provider can seek further clarification or supplementary information from the referring provider. The results generated by the referred provider should be uploaded directly to the patient's eHR for sharing with other healthcare providers providing care to the patient. This would not only ensure the completeness of the patient's eHR but also help avoid duplicated tests. To facilitate follow-up consultation by the referring provider on the results, the eHR Sharing System would flag up results that have not been reviewed by the referring provider.

4.17 We consider that the above mechanism could help achieve a balance between the referred providers' access to information on a "need-to-know" basis and under the "patient-under-care" principle, and the patients' convenience and privacy.

[20] A feature of the eHR Sharing System to facilitate referral of patients between healthcare providers.

### *Exemptions*

4.18 Personal data relating to the physical or mental health of a person are generally considered as sensitive data which should be carefully guarded against unlawful use and access. DPP3 stipulates that, without the consent of the data subject, his/her personal data should not be used for any purpose other than (i) the purpose for which the data were collected or (ii) a directly related purpose. However, as provided in Section 59 of PDPO, the right to protect such data relating to the physical or mental health of the data subject would have to give way when the strict compliance with DPP3 would be likely to cause serious harm to the physical or mental health of the data subject or any other individual.

4.19 In line with this provision, the eHR Sharing System will provide a special access feature for healthcare professionals to be exceptionally allowed to access the eHR of a patient for the specific purpose of delivering emergency care, without seeking prior consent from the patient. This special access will only be available to healthcare professionals who can justify its use in delivering emergency care. In defining situations which warrant such special access, reference will be made to Section 59 of PDPO to ensure consistent judgement of healthcare professionals. We would also put in place safeguard measures, for example the eHR Sharing System would log all such uses to monitor and report any misuse, and as stated in paragraph 4.61, send a notification to the subject patients on such access.

*Retention of eHR Upon Withdrawal/Expiry of Consent*

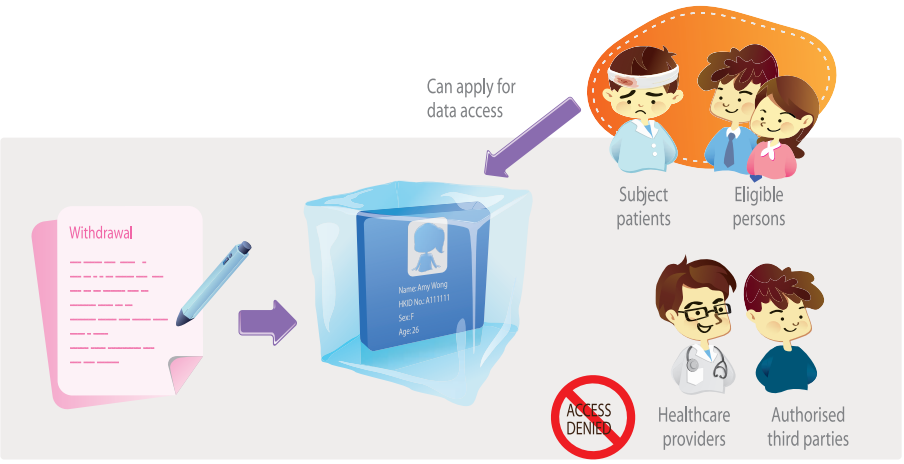


*Figure 10 – Withdrawal Arrangement*

4.20 Under the principle of voluntary participation, participants can withdraw from eHR sharing at any time. The eHR legislation should provide for the handling of the eHR of withdrawn patients and deceased patients. We propose that for a patient whose consent has expired due to his/her withdrawal or death, his/her eHR would be "frozen" (i.e. the record would not be available for access but remain in the eHR Sharing System) for a specified period. In line with DPP2(2) that data should not be kept longer than is necessary, the "frozen" eHR will be de-identified after the specified period.

4.21 In proposing the length of the specified "frozen" periods, we have considered the Limitation Ordinance (Cap.347) –

(a) Section 27(4) of the Limitation Ordinance provides that the time limit for taking civil actions in respect of personal injuries is three years from the date on which the cause of action accrued or the date of knowledge.

(b) Apart from that, the Limitation Ordinance sets out various limitation periods for representatives or executors to take civil actions in respect of damages to a deceased person, the longest being six years as stipulated in Section 22. Under Section 22, subject to certain conditions, if on the date when any right of action accrued for which a period of limitation is prescribed, the person to whom it accrued was under a "disability" (specifically defined as a minor or a person of unsound mind), an action[21] may be brought by the representative of the person at any time before the expiration of six years from the date when the person died.

4.22 We propose that the "frozen period" for withdrawn participants should be three years. Keeping the eHR of a withdrawn patient for three years also helps maintain the continuity of care in case the patient subsequently re-enrols. As regards the deceased patients, we consider it appropriate for the eHR Sharing System to retain their record for a longer period to provide for access by their representatives and for secondary uses. In this connection, the eHR of a deceased patient is suggested to be kept for ten years.

4.23 It is proposed that frozen eHR of withdrawn patients can only be accessed by the subject patient, or persons eligible to make a request for data access on behalf of the patient (see paragraphs 4.39-4.42 below). Frozen eHR of deceased patients can only be accessed by the administrator/executor or persons authorised by the Court. Overseas health legislation, such as Section 3(1)(f) of the United Kingdom's Access to Health Records Act 1990 provides similarly that only a deceased patient's personal representative, or any person who may have a claim arising out of the patient's death may apply for access to the patient's health records. Upon the withdrawal or death of the patient, any consent given by the patient to a healthcare provider for accessing and uploading data to his/her eHR will expire. To safeguard the privacy of withdrawn and deceased patients, the eHR Sharing System would completely de-identify all frozen eHR data as well as the archive and backup data of frozen eHR after the specified periods. De-identified eHR data will be retained in the eHR Sharing System for potential secondary uses (see paragraphs 4.35-4.36 below).

[21] This excludes action to which section 27 (related to personal injuries) or section 28(3) (related to actions under Fatal Accidents Ordinance (Cap.22) applies.

### *Re-enrolment Arrangement for Withdrawn Patients*

4.24 If a patient re-enrols after having withdrawn for more than three years, his/her frozen eHR would have been de-identified and the eHR Sharing System will have no record of the patient (including whether he/she has previously participated). As such, the re-enrolling patient will be treated as a new participant.

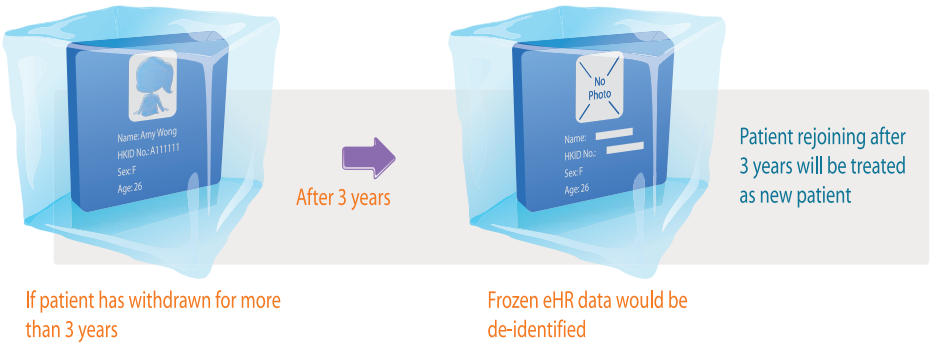


*Figure 11 – Rejoining Arrangement (Beyond three years of withdrawal)*

4.25 For a patient who re-enrols within three years of withdrawal, the eHR Sharing System would reactivate his/her eHR to preserve the completeness of the eHR. The re-enrolling patient may revalidate all consent previously granted to individual healthcare providers. After the revalidation, the eHR Sharing System will ask these healthcare providers to upload health data of the rejoining patients to the eHR Sharing System. These data would form the new eHR for the patients. We believe that this rejoining arrangement could best minimise the data loss of a rejoining patient as a result of their withdrawal.

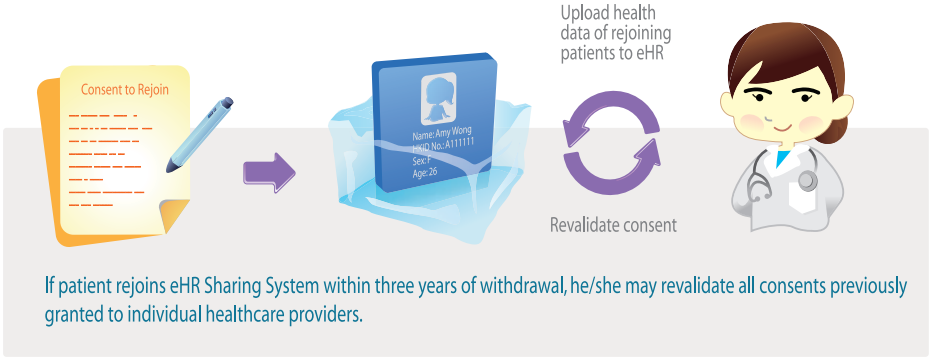


*Figure 12 – Rejoining Arrangement (Within three years of withdrawal)*

### *eHR Sharable Scope*

4.26 To ensure that participants have a clear idea of the information in the eHR, we should define the scope of the sharable eHR. In delineating the scope, we adopt the following principles –

(a) Only data necessary and beneficial for the continuity of healthcare should be included in the scope of eHR sharing;

(b) eHR information should be as complete and integral as possible to ensure the quality of healthcare. Hence, no safe deposit box (paragraphs 4.28-4.30) will be provided and no exclusion of eHR sharable data (paragraph 4.31) would be allowed.

4.27 Taking into account the clinical needs and to tie in with the technical capability of the eHR Sharing System, we propose that eHR sharable data should include in the first phase of development of eHR sharing –

(a) personal identification and demographic data;
(b) episodes/encounters with providers (summary);
(c) referral between providers;
(d) adverse reactions/allergies;
(e) diagnosis, procedures and medication;
(f) immunisation records;
(g) laboratory and radiology results; and
(h) other investigation results.

A full list of eHR sharable data to be covered under the scope by phases is at **Annex D**.

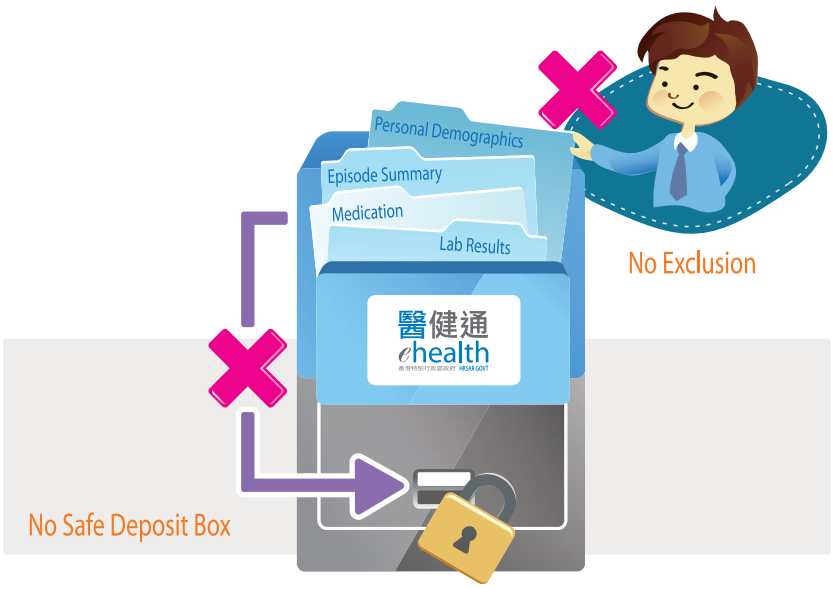


*Figure 13 – No Safe Deposit Box & No Exclusion*

*What is a safe deposit box?*

4.28 Safe deposit box is an electronic data feature which allows the separate storage of certain patient data with enhanced access control. In the context of eHR, this would mean allowing patients to prevent some categories of eHR sharable data from being automatically viewable by healthcare providers even with the general consent of the patients. Normally, the existence of such box would be indicated by a flag. Healthcare providers would need special consent for opening the box.

4.29 While recognising the sensitivity of some health data which would warrant extra safeguards, there is a need to balance extra protection for this sensitive data with the completeness and integrity of the eHR to ensure the quality of healthcare delivery.

4.30 We propose that there should not be a safe deposit box on grounds that –

(a) it would undermine the completeness of the eHR and the integrity of the eHR Sharing System and in turn affect the quality of healthcare;

(b) healthcare providers would need to know whether the data in the safe deposit box is clinically relevant to treatment, or points to extra caution in handling the patients (e.g. in case of infectious disease). This necessitates the concurrent access to the eHR and the information in the safe deposit box every time;

(c) it is practically difficult for healthcare professionals to determine which particular episodes can be regarded as sensitive health data to be stored separately in the safe deposit box. Apart from the names of illness/diseases, name of specialists, medications, etc. may all point to the health status of patients;

(d) the feature would add an extra layer of complexity to the design of the eHR sharing infrastructure and in turn impose extra administrative costs, both for developing and operating the eHR Sharing System; and

(e) there may also be a labelling effect on patients with a safe deposit box, since it is necessary to have their eHR flagged up.

*Exclusion*

4.31 We have also considered the possibility of allowing patients to choose to exclude certain eHR sharable data (say, hereditary diseases) from their eHR. However, this would similarly undermine the integrity and completeness of patients' eHR and affect the quality of care provided to patients. We therefore propose that participating healthcare providers will be required to make available health data in their eMR/ePRs falling within the eHR sharable scope for uploading to the eHR Sharing System and no exclusion would be allowed.

### *Copyright of the eHR Data*

4.32 Under the Copyright Ordinance (Cap.528), copyright in a document generally resides with the author. Data per se may not be eligible for copyright protection, but according to Section 4 of the Copyright Ordinance, a compilation of data which by reason of the selection or arrangement of its contents constitutes an intellectual creation may be eligible for copyright protection. Section 11 of the Copyright Ordinance provides that "author", in relation to a work, means the person who creates the work. Given the different ways in which patients' records are compiled by different healthcare providers, there are uncertainties as to the ownership of the copyright of eHR. To enable sharing and to have a clear delineation of responsibilities, we propose that under the Framework, any viewing, using or uploading of eHR data within the eHR Sharing System would not amount to copyright infringement.

### *Use of eHR Data*

#### *Primary Use*

4.33 The primary purpose of the collection and sharing of eHR data is to enhance the continuity of care for patients. The user agreement as mentioned in paragraph 4.7(a) would set out the terms and conditions of eHR sharing.

4.34 Healthcare providers participating in eHR sharing will be required to observe the relevant rules regulating the use of data available through the eHR Sharing System. Also, eHR Sharing System as an electronic platform would not be able to verify the completeness, truthfulness or accuracy of the eHR data uploaded by healthcare providers. Rather, these responsibilities would fall on the healthcare providers who contribute data to the eHR Sharing System. Healthcare providers should exercise their professional judgement when using eHR as a clinical reference, and seek clarification from the contributor of the eHR data if in doubts.

*Secondary Use*

4.35 The eHR Sharing System provides data for secondary uses such as public health research and disease surveillance. For example, eHR data may be used for infectious disease control as stipulated in the Prevention and Control of Disease Regulation (Cap.599A).

4.36 Section 62 of PDPO provides for the use of personal data without the express consent of data subjects for statistical and research purposes if the results are not made available in a form which identifies any of the data subjects. Notwithstanding this, we propose that research proposals for the use of non patient-identifiable eHR data for public health research and disease surveillance will require the approval of eHR-OB.

*Use of Patient-Identifiable Data*

4.37 In certain circumstances there may be wider public interest in the uses of patient-identifiable eHR data. To strike a balance between the public interest in these secondary purposes and the privacy of the participating patients and taking into account similar mechanism overseas[22], the Framework would provide that SFH may approve any proposal for the use of patient identifiable eHR data for public health research or disease surveillance, on the recommendation of a research board to be appointed by SFH, comprising of academics, patient representatives, DH, HA and relevant professional organisations. With reference to Section 44(3) of the Personal Health Information Protection Act, Ontario, Canada, the research board should consider issues such as –

(a) whether the research can be accomplished without the provision of the data requested;
(b) the public interest in the proposal;
(c) the practicality to obtain individual consent from data subjects; and
(d) whether there are adequate safeguards in place to protect the privacy of the data subjects.

[22] Such as the Research Ethics Board set up under Ontario's Personal Health Information Protection Act and Alberta's Health Information Act.

4.38 The eHR-OB and the research board should also give due consideration to the purpose of use and make reference to the secondary user's functions and activities before transferring the non patient-identifiable data to the secondary user or recommending the research proposals to SFH. In any case, the results of the research should not identify any subject patient. Secondary users should not have direct access to the eHR Sharing System. Instead, the required eHR data would be provided to them in bulk.

### *Data Access and Correction*

#### *Data Access Request (DAR)*

4.39 DAR is an important tool for individuals to access and check their own personal data. Section 18 of PDPO provides that any individual can make a DAR to be informed by a data user whether the data user holds his/her personal data, and if so, to obtain a copy of his/her personal data. Furthermore, PDPO provides that a "relevant person", i.e. a person with the parental responsibility for the minor, appointed by a court to manage the affairs of a person incapable of managing his/her own affairs, or authorised in writing by the individual, may make a DAR on behalf of the individual [23].

4.40 To facilitate patients' management of their own eHR, eHR-OB will comply with DARs made by the subject patients, persons with parental responsibility over minors, and guardians of MIPs. Other tools, such as the patient portal, are planned to be commissioned in the second stage of the eHR Programme to allow patients to access their own eHR more conveniently.

4.41 In line with our proposal that the age of majority in eHR sharing should be 16, persons with parental responsibility over minors under 16, instead of 18 as stated in the Interpretation and General Clauses Ordinance (Cap.1) and adopted in PDPO, should be allowed to make a DAR on behalf of the minors.

---

[23] Under the Personal Data (Privacy) (Amendment) Bill 2011, the Constitutional and Mainland Affairs Bureau has proposed to expand the definition of "relevant person" under Section 2 of PDPO to include the guardians of data subjects with mental incapacity, who are appointed under Sections 44A, 59O or 59Q of the Mental Health Ordinance (Cap.136), so that a more sufficient protection would be accorded to data subjects with mental incapacity with regard to the rights to complain and make data access and data correction requests.

4.42 The arrangement for authorised third parties to make DAR would not be implemented under the eHR Sharing System, due to the sensitivity of eHR data and the fact that the eHR Sharing System, as an electronic platform, would not be able to verify the authorisation of patients. As such, it is proposed that the eHR legislation should stipulate that only the data subject, the persons with parental responsibilities over minors and guardians of MIP could make a DAR to eHR-OB.

### *Fee Charged for DAR*

4.43 Current provisions in PDPO stipulate that custodians may charge a fee which is not excessive to comply with a DAR. In this connection, we will stipulate under the eHR legislation that a fee will be charged for making available the eHR in compliance of a DAR and will deliberate an appropriate fee level. As minimal administration would be required for the eHR Sharing System to produce the patient's eHR, we envisage that this fee would be lower than what healthcare providers currently charge for patients' records in paper form.

### *Data Correction*

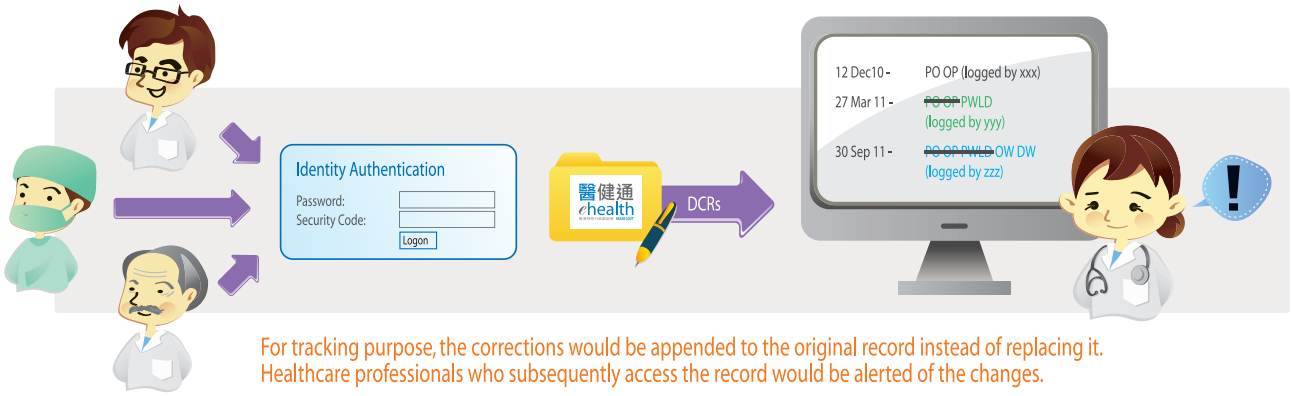


***Figure 14 – Data Correction Request***

4.44 Pursuant to Section 22 of PDPO, a patient can request correction on his/her eHR data. We consider that persons allowed to make a DAR to eHR-OB should also be allowed

to make a data correction request (DCR) regarding eHR data. However, since eHR-OB does not contribute any health data and is therefore not in a position to verify whether a correction is justified, we will set out in the eHR legislation and/or the COP that any DCR made by the patient, person with parental responsibility over minors, or guardian of MIPs to eHR-OB will be handled by the healthcare provider which uploaded the data concerned. If the healthcare provider does not agree with the patient that the eHR data concerned is inaccurate, he/she may refuse to correct the data, but should make a note of the matters in respect of which eHR data is considered by the patient to be inaccurate[24]. This note would become part of the patient's eHR and available to other healthcare providers so that they may exercise their own professional judgement when viewing the eHR.

4.45 Healthcare providers may also wish to rectify errors spotted in the eHR data they uploaded. The existing professional codes of conduct, for example, Section 1.1.3 of the Code of Professional Conduct for Registered Medical Practitioners[25], stipulates that all doctors have the responsibility to maintain systematic, true, adequate, clear, and contemporaneous medical records. In line with the current practice, they would be allowed to amend an eHR (excluding PMI data) as necessary without having to seek the subject patient's prior consent. However, we would make clear in the Framework that healthcare professionals should assess the impact of each amendment and exercise their professional judgement to determine if the subject patient should be notified on an amendment.

4.46 To track all amendments made in eHR, the original data would not be overwritten when an amendment is made. Rather, the amendment would be appended to the original record. Besides, the eHR Sharing System would highlight the changes/ corrections made in a mark-up/tracking mode so that healthcare providers who subsequently access the data will have a better understanding of the patient's medical history. This is important as the eHR serves only as a clinical record for reference, and it is possible that different healthcare professionals may have different opinions. In summary, it is suggested that the eHR Sharing System and healthcare providers would need to -

[24] Reference is made to section 25(2) of PDPO.
[25] http://www.mchk.org.hk/code.htm

(a) identify and authenticate the patient or the person making a DCR;

(b) identify and authenticate the authorised person amending the eHR data;

(c) be able to trace the amendment and the person making it; and

(d) alert healthcare providers who subsequently access the eHR of the changes made in the patient's eHR.

### *Complaint and Review Mechanism*

4.47 Currently, PDPO sets out mechanisms for data subjects to make a complaint in relation to an act which is suspected to have contravened the relevant legislations[26]. We also note that the relevant legislation of Canada stipulates the mechanism to request a review on decisions of data users[27] when a data user refuses to comply with a DAR. In this connection, we will formulate a similar mechanism to initiate review and resolve complaints arising from eHR sharing under the Framework. This is to allow complaints to be made and reviews to be initiated on data privacy and security matters relating to the access to and use of eHR data, or the eHR Sharing System.

### *Criminal Sanctions*

4.48 Existing legislation, such as the Telecommunications Ordinance (Cap.106) and the Crimes Ordinance (Cap.200), has provisions which criminalise unauthorised access to, and dishonest use of computer systems. They would offer certain deterrent against breach of data privacy and system security in the eHR Sharing System. However, as such breach would not only intrude the privacy of the patients, but also pose a significant threat to a large number of patients' lives if their eHR are maliciously edited, we consider it necessary to create in the eHR legislation new criminal offences which provide stronger deterrent against unauthorised access to the eHR Sharing System with a malicious intent. The sanction level

[26] Section 37 of PDPO

[27] Section 73 of the Health Information Act, Alberta, Canada

will be considered with reference to existing legislation (details at **Annex E**) and the new offence proposed by the Constitutional and Mainland Affairs Bureau in the Personal Data (Privacy) (Amendment) Bill 2011[28]. The Framework does not intend to criminalise health-care professionals or healthcare providers for innocent errors made in inputting eHR data or other unintentional contraventions in their delivery of healthcare to patients. Apart from criminal sanctions, patients who suffered from a contravention of a PDPO requirement may still seek remedies through the civil provisions set out in Section 66 of PDPO.

### *COP, Guidelines and Security Audits*

4.49 As mentioned in paragraph 4.4 above, we would govern the operation of the eHR Sharing System and regulate the access to the eHR Sharing System by healthcare providers, to ensure their compliance with the privacy and security standards and to enforce the necessary safeguards to uphold the protection of patients' privacy. To this end, while making the system sufficiently versatile and technology neutral to cater for future advancement in technology, we consider it best that eHR-OB may by way of publishing operating guidelines, best practices, procedural standards and/or other forms of guidelines regulate how individual eMR/ePR systems should operate and behave, and how interconnection with and access to eHR Sharing System should be made.

### *COP*

4.50 Under the Framework, we propose eHR-OB should be empowered to issue and maintain a COP which would bind healthcare providers that their eMR/ePR systems are required to comply with the relevant security requirements. The COP would set out the rules and regulations on participating healthcare providers' internal access procedures and control, as well as the security standards and requirements that their eMR/ePR systems must meet. The COP would be updated regularly to ensure that patient's eHR remains duly

[28] The Constitutional and Mainland Affairs Bureau has proposed under the Personal Data (Privacy) (Amendment) Bill 2011 that any person who discloses personal data of a data subject which was obtained from a data user without the data user's consent with an intent to obtain gain in money or other property or with an intent to cause loss in money or other property or with the result of causing psychological harm to the data subject will commit an offence and be liable, on conviction, to a fine of $1,000,000 and imprisonment for five years.

protected in tandem with technological advancements. Non-compliance with the COP per se may not lead directly to legal liability under the eHR legislation. However, eHR-OB should be backed by specific authority under the eHR legislation, such that where breach of data privacy or system security is found in case of review of complaints, security checks or audits, eHR-OB may require remedial actions to be taken by users and managers of individual eMR/ePR systems in compliance with the COP and terminate access by the concerned healthcare providers until the requested remedial actions have been taken.

### *Security and Privacy Safeguards*

4.51 We propose that under the COP, a certification scheme would be developed to ensure the conformity of individual eMR/ePR systems with the interoperability and security standards set out by eHR-OB so as to ensure the reliable and secure sharing of eHR between the individual eMR/ePR systems through the eHR Sharing System. Under the certification scheme, guidelines on the design of individual eMR/ePR systems would be mapped out. An eHR certification body/agent will certify the compliance of eMR/ePR system of a healthcare provider with these guidelines and the required security standards before allowing it to participate in eHR sharing and interconnect with eHR Sharing System. Participating healthcare providers may only access and upload eHR data to the eHR Sharing System through certified eMR/ePR systems.

### *Authentication of Patients and Healthcare Providers*

4.52 Currently, healthcare providers would exercise due diligence to authenticate the identity of the visiting patient during consultation, in particular MIPs and minors to ensure that the medical record is rightly attributed to that patient. While healthcare providers' responsibility remains unchanged under eHR sharing, the eHR Sharing System will provide various means to buttress the authentication and reduce potential errors in the process, such as the electronic use of the patients' Smart ID card. A PMI will be centrally maintained by the eHR Sharing System to uniquely identify and attribute eHR data to individual patients. PMI data, including the Chinese and English names of the patient, his/her identity document number, date of birth, sex, address, mobile number, etc., forms an identification of the patient which is necessary for authentication and clinical record management.

4.53 To ensure the correct attribution of eHR data to the subject patient and that only authorised persons may access the eHR Sharing System, we propose that the eHR Sharing System will –

(a) authenticate the identity of healthcare providers through certifying their eMR/ePR systems or other means;

(b) register healthcare professionals participating in eHR sharing to a central healthcare professional database, and authenticate individual healthcare professionals through this database to verify their professional registration and facilitate role-based access control (paragraphs 4.54-4.55);

(c) require participating healthcare providers to design an appropriate role-based access control for their own eMR/ePR systems;

(d) bar healthcare providers from access to a patient's eHR upon the expiry of the one-year consent, the revocation of consent or the death of the patient; and

(e) require healthcare providers to exercise due diligence to authenticate the identity of visiting patients, including MIPs and minors.

*Role-based Access Control for Healthcare Professionals*

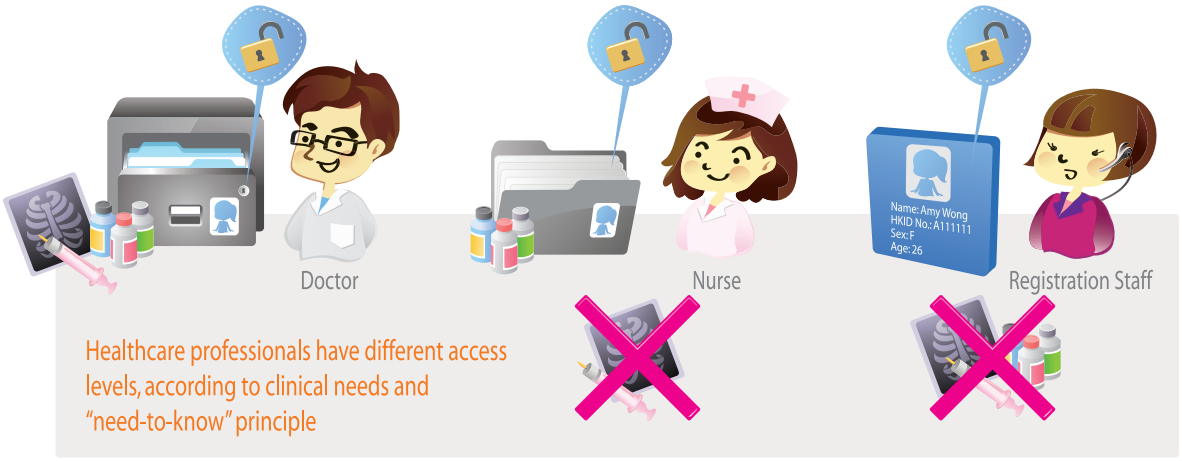


*Figure 15 – Role-based Access Control*

4.54 A healthcare professional may not be automatically granted access to a patient's entire eHR. To implement the "need-to-know" principle and ensure that healthcare professionals have access to parts of eHR relevant to their professional service, we propose that the healthcare provider should implement a role-based access control with pre-defined differentiated access rights set in accordance with the clinical need or function of different healthcare professionals. For example, a doctor may be granted access to the entire eHR, and the right to view and upload a prescription; whereas a registered nurse may only have access to certain parts of the eHR, and the right to view but not upload a prescription.

4.55 It is proposed that the eHR Sharing System will set up a central registry for various healthcare professionals. When a healthcare professional accesses an eHR through his/her eMR/ePR system, he/she will be authenticated against this central database. Once authenticated, the eHR Sharing System would grant appropriate access right to eHR in accordance with his/her profession and role assigned by the healthcare provider. This two-tier control mechanism (at the healthcare provider level and eHR Sharing System level) could ensure that the patient's eHR is only accessed by the healthcare professionals delivering care to them.

### *Validation and Proof of Integrity and Origin of eHR Data*

4.56 The eHR Sharing System will adopt appropriate data privacy and security guidelines and procedures from PCPD, the Office of the Government Chief Information Officer, and relevant experience both in Hong Kong and overseas. Consultancy study on IT security and audit framework had been commissioned to make recommendations on security and control mechanisms. Relevant security measures will be built into different levels of the eHR Sharing System. Network security mechanisms, e.g. firewalls, intrusion detection tools will be in place to guard against Internet attacks.

4.57 The eHR Sharing System would establish a mechanism to ensure the quality of the data in the System and non-repudiation[29] of acts on such data. To ensure the quality of data uploaded, the eHR Sharing System will perform data validation on any data being imported to the System as far as possible. For example, the eHR Sharing System will validate important patient demographic data, e.g. Hong Kong Identity Card number, date of birth and sex to avoid inputting errors. In the case of a drug code, the System will verify if it is a valid code in the drug table. However, for scanned images and free format text input, the System could not perform any validation.


*Figure 16 – Data Validation*

[29] In the context of eHR, non-repudiation means that a person uploading or correcting eHR data would not be able to deny having done so, since all acts and the persons committing the act will be recorded.

4.58 The eHR Sharing System may implement appropriate security features (e.g. digital certification) to provide proof of integrity and origin of eHR, so that the healthcare providers would not be able to deny their act of uploading or amending certain eHR data. The eHR Sharing System would also encrypt eHR data in the databases, files, archives, and during transmission as appropriate and implement access control against unauthorised access.


*Figure 17 – Data Encryption During Transmission*

### *Downloading of Defined Set of eHR*

4.59 Many security incidents have arisen from the downloading of personal data to portable devices which are subsequently lost. To prevent data leakage, downloading of eHR data from the eHR Sharing System would be restricted. As an initial proposal, only data in the PMI data and allergy/adverse reaction information can be downloaded from the eHR Sharing System. Allergy information is essential to vital clinical decision support as healthcare professionals should be alerted if the medication they prescribe may trigger an adverse reaction.

4.60 Other eHR data, such as diagnosis and episode summary, can only be viewed from the eHR Sharing System, but not downloaded. This is to minimise the risk of leakage through healthcare providers' eMR/ePR systems or printed records.

### *Access Notification*

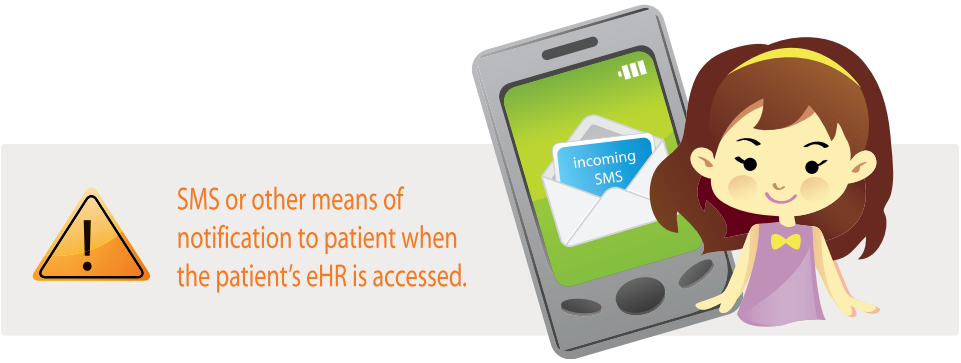


*Figure 18 – Patient Notification*

4.61 To facilitate the reporting of suspected unauthorised access/use of eHR data, the eHR Sharing System will notify the patient, via a Short Message Service or other means, when his/her eHR is accessed. Patient notification may be sent in the following scenarios -

(a) access to patient's eHR with the patient's or the SDM's consent;

(b) expiry of patient's express consent to a healthcare provider and any subsequent attempt to access the patient' eHR by this healthcare provider;

(c) access to patient's eHR without consent under exceptional circumstances (e.g. under emergency situations); and

(d) security concerns that may affect subject patients' eHR.

### *Access Logging*

4.62 To facilitate necessary access control and audits, participating healthcare providers will be required to maintain accurate and up-to-date logs on any access to eHR made through their eMR/ePR systems. The eHR Sharing System would also record the access by the healthcare providers and healthcare professionals under role-based control of the healthcare providers. The log of eMR/ePR may include the following information -

(a) the identity of patient whose eHR is accessed;

(b) the identity of the healthcare professional accessing the eHR;

(c) the date and time of access made;

(d) whether access is made with patient's consent, substitute consent, or without consent (e.g. under emergency situations);

(e) if substitute consent is obtained, the identity of SDM; and

(f) if a change to patient's eHR is made, whether patient's consent or substitute consent is obtained.

The healthcare providers will need to provide their access logs to relevant authorities upon request.

### *Editing the PMI Data of Patients*

4.63 Certain security safeguards such as authentication in the eHR Sharing System rely on the PMI data of the patient, such as the mobile phone number for access alert to patients. To prevent circumvention of these security safeguards and the PMI data from malicious tampering, it is proposed that healthcare providers would require patient's consent to edit the PMI data on the patient's behalf.

4.64 The above security and privacy safeguards are by no means exhaustive. These would be further refined in the preparation of the COP and in the light of the findings of the Security Risk Assessment and PIA.

### *Security Monitoring and Audit*

4.65 As a preventive measure to detect violations of COP, unauthorised accesses, or other security breaches, healthcare providers would be required to perform regular audits on their own eMR/ePR systems. Any security breaches or loopholes should be promptly mitigated and reported to eHR-OB as appropriate. To ensure compliance and as a check and balance, eHR-OB should be empowered to perform security audits on the eMR/ePR systems and on the internal access control of healthcare providers, both of which may be performed at random pick or on account of complaint, and suggest mitigating measures for healthcare providers which do not conform fully to COP. As mentioned in paragraph 4.62, participating healthcare providers should log all access to the eHR Sharing System through their eMR/ePR systems to facilitate these regular or random audits.

4.66 Regular security audits would also be conducted on the eHR Sharing System to ensure its safe and secure operation. In addition, the eHR Sharing System would implement a number of protection features against security breaches through continuous system monitoring to identify any irregular patterns in the use of eHR data, such as frequent access to a large number of patient records, extensive amendments, and other identifiable irregularities. These irregularities will be brought to the attention of eHR-OB, which will assess if further investigation is required. Such active monitoring would help prevent or stop unauthorised access to the eHR Sharing System as soon as possible to safeguard against intrusion to patient's privacy.

### *Handling of Privacy and Security Breaches*

4.67 Despite all the necessary safeguards, we need to prepare for any security breaches. In case of such breaches, eHR-OB will notify patients as mentioned in paragraph 4.61, and follow the mechanism set down in the prevailing government guidelines for handling information security incidents. For example, Government Bureaux and Departments are expected to report any security incident involving personal data to PCPD as soon as possible and notify affected individuals as far as practicable. In addition, healthcare providers should notify eHR-OB in the event of a security breach in their eMR/ePR systems.

4.68 There is currently no security incident reporting mechanism specified in PDPO. In this regard, PCPD promulgated a guidance note entitled "Data Breach Handling and the Giving of Breach Notifications" to assist data users in handling data breaches and to facilitate them in giving data breach notifications[30]. As mentioned in the guidance note, data breach notifications would draw the affected data subjects' attention to take appropriate protective measures, allow relevant authorities to undertake appropriate follow up actions, and increase public awareness. We would further deliberate the notification system and information to be included in the eHR security breach notification in accordance with PCPD's guidance note. Given the speed at which eHR data can be further disseminated or used, the technical design of the eHR Sharing System should include some automatic blocking/access bar functions to contain any potential damages of the security breaches. System alerts to healthcare providers/patients should also be built in. These requirements would be further deliberated during the design stage.

4.69 The above sets out the proposed Framework and the consideration behind. Subject to the results of the consultation, we may need to refine the Framework and map out the implementation details in the eHR legislation as well as the COP.

[30] http://www.pcpd.org.hk/english/publications/files/DataBreachHandling_e.pdf

# *Chapter 5: Way Forward*

5.1 The global healthcare sector is anticipating a huge breakthrough – the integration of healthcare services and information technology realised in eHR sharing. Apart from Hong Kong, many countries, such as Canada, Australia, Singapore, Sweden, Denmark, just to name a few, are pursuing eHR projects in earnest. Once completed, Hong Kong's territory-wide, patient-oriented eHR Sharing System will benefit healthcare providers and patients by allowing standardised eHR to be accessed, updated and shared by healthcare providers, in a timely, secure and comprehensive way.

## We Need Your Views

5.2 We would like to express our gratitude to your support to the proposal to develop the eHR Sharing System in the first stage public consultation on healthcare reform in 2008. To take the proposal forward, the invaluable contribution from experts and key stakeholders is highly appreciated, but what count the most are the views from all of you. We would like to seek your views on the proposed Framework as set out in Chapter 4 of this document. In particular, we would like to know if you agree to the following proposals, or if you would have other suggestions –

(a) Voluntary participation – Patients and healthcare providers would participate in eHR sharing on a voluntary basis; and individual healthcare providers would need to obtain the express and informed consent of patients for accessing and uploading of data to the patients' eHR. (paragraph 4.4(a))

(b) Validity of consent – Patients' consent to an individual healthcare provider would cover future eHR access or referrals by that specific healthcare provider, and may be either "one-year" or "open-ended until revocation". Consent for HA and DH to access a patient's eHR should be part and parcel to the enrolment to eHR sharing. (paragraphs 4.7 and 4.10)

(c) SDM – Minors under 16 or other patients unable to give an informed consent may join eHR sharing with the substitute consent of an SDM. An SDM may be a person with parental responsibilities over minor, a person appointed by the Court or the Guardianship Board, an immediate family member or a healthcare provider delivering care in the best interest of a patient. (paragraphs 4.11 to 4.13)

(d) Exemptions – Under exceptional circumstances (e.g. delivery of emergency care) eHR data may be accessed by healthcare providers without the subject patient's consent. (paragraph 4.18 to 4.19)

(e) eHR of withdrawn or deceased patients – The eHR data of withdrawn or deceased patients will be kept for three years or 10 years respectively before being de-identified. (paragraphs 4.20 to 4.23)

(f) The proposed eHR sharable scope – No "safe deposit box" and no exclusion. (paragraph 4.26 to 4.31)

(g) Use of eHR data – The primary use of eHR data is for the continuity of care of patients. Secondary uses of eHR data for public health research and surveillance would be subject to the approval of the eHR-OB or the SFH. (paragraphs 4.33 to 4.38)

(h) Data access and correction – For better protection of the patients' privacy, only subject patient, person with parental responsibilities over minor, and guardian of MIP appointed by Court can make a DAR or a DCR to eHR-OB. Any amendments would be marked in tracking mode. (paragraphs 4.39 to 4.46)

(i) Criminal sanctions – A stronger deterrent against unauthorised access to the eHR Sharing System with malicious intent would be introduced through the eHR legislation. (paragraph 4.48)

(j) Various security measures on eHR data – These include, among others –

(i) COP – The regulation of the healthcare provider's access will be governed by a COP to be developed by the eHR-OB under the eHR legislation, which would set out the internal access control rules and regulations as well as the security standards and requirements of the healthcare provider's system (paragraph 4.50);

(ii) role-based access control – Authentication of patients and healthcare providers and role-based access control for healthcare professionals with checks against a central professional registry would be implemented (paragraphs 4.52 to 4.55);

(iii) data encryption, data validation, proof of integrity and origin of eHR data (paragraphs 4.56 to 4.58);

(iv) limited downloading of eHR data – Only PMI data and allergy information, which are necessary for clinical record management and decision support, may be downloaded from the eHR Sharing System (paragraph 4.59 to 4.60); and

(v) handling of privacy and security breaches – Notifications and alerts in the event of privacy or security breaches would be put in place. Automatic blocking/access bar functions would be built into the eHR Sharing System to contain any potential damage caused by such breaches (paragraphs 4.67 to 4.68).

5.3 It is only through your participation that we can develop an effective, efficient and sustainable system to share health records according to your needs. We also hope that both public and private stakeholders in the community would be ready to embrace the changes to healthcare service to be brought about by eHR sharing.

5.4 We are consulting the public on the Framework and welcome your views which would be instrumental to the success of the eHR Sharing System. Please send us your views on this consultation document **on or before 11 February 2012** via the contact below. Please let us know if you do not want your views to be published, or if you wish to remain anonymous when your views are published. Unless otherwise specified, all responses will be treated as public information and may be published in future.

| | |
|---|---|
| Address: | Electronic Health Record Office<br>Food and Health Bureau<br>19/F, East Wing, Central Government Offices<br>2 Tim Mei Avenue, Tamar, Hong Kong |
| Fax: | (852) 2102 2570 |
| Email: | eHR@fhb.gov.hk |
| Website: | www.ehealth.gov.hk |

## *eHR Legislation*

5.5 Based on your views raised during the consultation, we will refine the Framework and proceed to draft the eHR legislation, which will help safeguard the interests of both patients and healthcare providers, and allow the eHR Sharing System to function effectively and in a secured manner.

# *Annex A: Steering Committee on eHealth Record Sharing*

## Membership List

Chairperson: Mr Richard YUEN, Permanent Secretary for Food and Health (Health)
Secretary: Mr Michael YAU, Administrative Officer (eHealth Record)1

| Organisation | Name | Post Title |
|---|---|---|
| Food and Health Bureau | Mr Richard YUEN, JP | Permanent Secretary for Food and Health (Health) |
| | Mr Michael YAU | Administrative Officer (eHealth Record)1 |
| Department of Health | Dr Gloria TAM, JP | Deputy Director of Health |
| | Dr Heston KWONG | Assistant Director of Health (Special Health Services) |
| Hospital Authority | Mr Andre GREYLING | Chief Information Officer |
| | Ms Christina CHENG | Cluster General Manager (Finance), Kowloon Centre Cluster |
| Office of the Government Chief Information Officer | Mr MAK Hung Sung Stephen, BBS, JP | Government Chief Information Officer |
| | Mr Victor LAM | Deputy Government Chief Information Officer (Consulting and Operations) |
| | Miss Joey LAM, JP (Alternative member) | Deputy Government Chief Information Officer (Policy and Customer Service) |
| Hong Kong Academy of Medicine | Dr Gene TSOI | Immediate Past President of The Hong Kong College of Family Physicians |
| | Dr Louis WC CHOW | Honorary Secretary |
| Hong Kong Private Hospitals Association | Dr Alan LAU | Chairperson |
| | Ms Manbo MAN | Director of Nursing Services Hong Kong Sanatorium & Hospital |

## Annex A: Steering Committee on eHealth Record Sharing

| Organisation | Name | Post Title |
|---|---|---|
| ***ad personam*** | Dr Lincoln CHEE | Chief Executive Officer<br>Quality Healthcare Asia Limited |
| ***ad personam*** | Dr Roy CHO Kwai-chee | Executive Director<br>Town Health |
| Hong Kong Medical Association | Dr TSE Hung-hing | Immediate Past President |
| | Dr HO Chung-ping, MH, JP | Council Member |
| Hong Kong Doctors Union<br>(until August 2011) | Dr Alfred TANG Kuen-yan | Council Member |
| | Dr Eric TANG Wai-choi | Council Member |
| Hong Kong Public Doctors' Association | Dr HO Pak-leung | Member |
| ***ad personam*** | Dr Eric CHAN | Senior Manager (Nursing)/<br>Principal Nursing Officer<br>Hospital Authority |
| ***ad personam*** | Mr Lawrence FUNG | Department Manager<br>(Physiotherapy)<br>Kwong Wah Hospital |
| Alliance for Renal Patients Mutual Help Association | Mr Andy LAU | Chairperson |
| Care For Your Heart - Cardiac Patients Mutual Support Association | Mr Jeff LEE | Vice Chairperson |
| Alliance for Patients Mutual Help Organisations | Mr TSANG Kin-ping | Chairperson |
| | Dr Margaret CHUNG | Founding Member |

# *Annex B: Working Group on Legal, Privacy and Security Issues*

## Membership List

Chairpersons: Miss Janice TSE, Head (eHealth Record)
Dr N T CHEUNG, Consultant (eHealth)
Secretary: Mr Christopher NUNG, Administrative Officer (eHealth Record)2

| Organisation | Name | Post Title |
|---|---|---|
| Food and Health Bureau | Miss Janice TSE | Head (eHealth Record) |
| | Dr N T CHEUNG | Consultant (eHealth) |
| | Mr Christopher NUNG | Administrative Officer (eHealth Record)2 |
| Department of Health | Dr Liza TO | Principal Medical and Health Officer (4) |
| Office of the Government Chief Information Officer | Miss Donna CHAN | Chief Systems Manager (IT Strategy) (IS) |
| | Mr Terence TSE | Senior Systems Manager (Business Transformation) 10 |
| Hospital Authority | Ms Christina CHENG | Cluster General Manager (Finance), Kowloon Central Cluster |
| | Ms Venus CHOY | Chief Legal Counsel |
| Office of the Privacy Commissioner for Personal Data, Hong Kong | Ms Brenda KWOK | Deputy Privacy Commissioner for Personal Data (Acting) |
| Consumer Council | Mr Simon CHUI | Senior Legal Counsel |
| Hong Kong Medical Association | Dr CHENG Chi-man | Council Member |
| Hong Kong Doctors Union (until August 2011) | Dr Alfred TANG Kuen-yan | Council Member |
| | Dr Eric TANG Wai-choi | Council Member |

## Annex B: Working Group on Legal, Privacy and Security Issues

| Organisation | Name | Post Title |
|---|---|---|
| Internet Professional Association | Mr Kenny CHIEN | Executive Committee Member |
| Alliance for Renal Patients Mutual Help Association | Mr Andy LAU | Chairperson |
| Care For Your Heart – Cardiac Patients Mutual Support Association | Mr Jeff LEE | Vice Chairperson |
| Alliance for Patients Mutual Help Organisations | Mr TSANG Kin-ping | Chairperson |
| | Dr Margaret CHUNG | Founding Member |
| ***ad personam*** | Dr CHAN Chun-man | Specialist in Emergency Medicine<br>Queen Elizabeth Hospital |

# *Annex C: Data Protection Principles under the Personal Data (Privacy) Ordinance (Cap.486)*

## 1. Principle 1 - purpose and manner of collection of personal data

(1) Personal data shall not be collected unless-

(a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and

(c) the data are adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are-

(a) lawful; and

(b) fair in the circumstances of the case.

(3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that-

(a) he is explicitly or implicitly informed, on or before collecting the data, of-

(i) whether it is obligatory or voluntary for him to supply the data; and

(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed-

(i) on or before collecting the data, of-

(A) the purpose (in general or specific terms) for which the data are to be used; and

(B) the classes of persons to whom the data may be transferred; and

(ii) on or before first use of the data for the purpose for which they were collected, of-

(A) his rights to request access to and to request the correction of the data; and

(B) the name and address of the individual to whom any such request may be made,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

## 2. Principle 2 - accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that-

(a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;

(b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used-

(i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data are erased;

(c) where it is practicable in all the circumstances of the case to know that-

(i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and

(ii) that data were inaccurate at the time of such disclosure, that the third party-

(A) is informed that the data are inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

### 3. Principle 3 - use of personal data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than-

(a) the purpose for which the data were to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a).

### 4. Principle 4 - security of personal data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorised or accidental access, processing, erasure or other use having particular regard to-

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data are stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

### 5. Principle 5 - information to be generally available

All practicable steps shall be taken to ensure that a person can-

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user are or are to be used.

## 6. Principle 6 - access to personal data

A data subject shall be entitled to-

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data-

  (i) within a reasonable time;

  (ii) at a fee, if any, that is not excessive;

  (iii) in a reasonable manner; and

  (iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

# *Annex D: Proposed Scope of Sharable eHR Data*

| eHR Content | Definition | Phase 1 | Later Phases |
|---|---|---|---|
| Person demographics | All information that is required to accurately and uniquely identify a person, including -<br>• eHR person identifier<br>• identity data<br>• demographic data<br>• next-of-kin data<br>• mother-baby linkage (for newborn baby) | ✓ | ✓ |
| Encounters | A list of booked appointments and attended healthcare encounters (face-to-face or electronic contact between a person and the healthcare practitioner who will assess, evaluate and treat a person). An episode is composed of one or more encounter(s). | ✓ | ✓ |
| Referral | Information that is required when a health-care practitioner transfers all or a portion of a person's care to another healthcare practitioner. | ✓ | ✓ |
| Episode summary | Information that summarise the following -<br>• Reason originating the episode and the person condition during initial encounter<br>• Major diagnostic findings during the course of the episode<br>• Problems identified<br>• Significant procedures performed and other related therapeutic treatment, e.g. medication<br>• The person's condition, therapeutic orders or treatment plan while preparing a periodic episode summary or upon termination of an episode<br>• Follow-up arrangement<br>• Education to the person/family, if applicable | ✓ | ✓ |
| Adverse reactions/ allergies | Information on the type of biological, physical or chemical agents that would result in/is proven to give rise to adverse health effects. Details of the adverse reactions, if occurred, should also be included. | ✓ | ✓ |

# Annex D: Proposed Scope of Sharable eHR Data

| eHR Content | Definition | Phase 1 | Later Phases |
|---|---|---|---|
| Problems | All active and inactive significant health and social problems. A problem can be a diagnosis, pathophysiological state, significant abnormal physical sign and examination finding, social problem, risk factor, allergy, reaction to drugs or foods, or health alert. | ✓ | ✓ |
| Procedures | Any significant procedures that are done for diagnosis, exploratory or treatment purposes. | ✓ | ✓ |
| Assessment/ physical exam | Observation made on a particular person after a systematic examination which is usually done according to body part, and also body system as assessment/physical examination. | | ✓ |
| Social history | Information about the lifestyle practices that may directly or indirectly affect a person's health, e.g. occupation, travel, hobbies, habits, etc. | | ✓ |
| Past medical history | Prior illnesses, injuries, treatment received which may or may not have an effect on the current care. | | ✓ |
| Family history | Hereditary or contact diseases that occurred in the family. | | ✓ |
| Medication | This includes medication ordered and/or dispensed/administered during the health-care process. | ✓ | ✓ |
| Immunisation | All vaccines administered to the person. | ✓ | ✓ |
| Clinical request | The health intervention that a practitioner instructed for the diagnosis/treatment of a person, e.g. laboratory investigation, radiology examination, or allied health service. | | ✓ |
| Laboratory results | Result of the laboratory tests which are subclassified according to the nature of the test, namely anatomical pathology, biochemistry, haematology, microbiology, virology, and other laboratory test. | ✓ | ✓ |

# Annex D: Proposed Scope of Sharable eHR Data

| eHR Content | Definition | Phase 1 | Later Phases |
|---|---|---|---|
| Radiology results | Radiology results would include radiology report and images. They are subclassified according to modality, e.g. plain x-ray, fluoroscopy, ultrasound, computer tomography, magnetic resonance imaging, nuclear medicine, angiography and vascular interventional radiography, non-vascular interventional radiography, positive emission tomography and others. | ✓ (textual reports) | ✓ (reports and images) |
| Other investigation results | Other diagnostic test results could be of diverse range as discrete data element or a full report of the diagnostic test. Images, e.g. clinical photos, tracing, could also be included. | ✓ | ✓ |
| Care and treatment plan | All planned/scheduled clinical requests, appointments, referrals, procedures, education and/or services that a healthcare practitioner considers that would aid in the diagnosis of/treatment to a person. | | ✓ |

# *Annex E: Existing Sanctions in Hong Kong Legislation*

**Chapter: 106 TELECOMMUNICATIONS ORDINANCE**
**Section: 27A Unauthorised access to computer by telecommunications**

(1) Any person who, by telecommunications, knowingly causes a computer to perform any function to obtain unauthorised access to any program or data held in a computer commits an offence and is liable on conviction to a fine of $20000. (Amended 36 of 2000 s. 28)

(2) For the purposes of subsection (1) -

(a) the intent of the person need not be directed at-
  (i) any particular program or data;
  (ii) a program or data of a particular kind; or
  (iii) a program or data held in a particular computer;

(b) access of any kind by a person to any program or data held in a computer is unauthorised if he is not entitled to control access of the kind in question to the program or data held in the computer and -
  (i) he has not been authorised to obtain access of the kind in question to the program or data held in the computer by any person who is so entitled;
  (ii) he does not believe that he has been so authorised; and
  (iii) he does not believe that he would have been so authorised if he had applied for the appropriate authority.

(3) Subsection (1) has effect without prejudice to any law relating to powers of inspection, search or seizure.

(4) Notwithstanding section 26 of the Magistrates Ordinance (Cap 227), proceedings for an offence under this section may be brought at any time within 3 years of the commission of the offence or within 6 months of the discovery of the offence by the prosecutor, whichever period expires first. (Added 23 of 1993 s. 2)

**Chapter: 200 CRIMES ORDINANCE**
**Section: 161 Access to computer with criminal or dishonest intent**

(1) Any person who 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 for himself or another; or

(d) with a dishonest intent to cause loss to another,

whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.

(2) For the purposes of subsection (1) "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 loss by parting with what one has.

(Added 23 of 1993 s. 5)

**Chapter: 486 PERSONAL DATA (PRIVACY) ORDINANCE**
**Section: 64 Offences**

## PART IX
## OFFENCES AND COMPENSATION

(1) A data user who, in any -

(a) data user return submitted under section 14(4) to the Commissioner;

(b) notice under section 14(8) served on the Commissioner; or

(c) notice under section 15(3) or (4) submitted to or served on the Commissioner, knowingly or recklessly supplies any information-
(i) which is false or misleading in a material particular; and
(ii) in purported compliance with that section, commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.

(2) A person who, in any data access request or data correction request, supplies any information-

(a) which is false or misleading in a material particular; and

(b) which is so supplied for the purpose of having the data user concerned comply with the request, commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.

(3) A person who, in any notice under section 15(6) served on the Commissioner, supplies any information-

(a) which is false or misleading in a material particular; and

(b) which is so supplied for the purpose of having the Commissioner comply with the request to which the notice relates, commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.

(4) A data user who, in any matching procedure request submitted to the Commissioner, supplies any information-

(a) which is false or misleading in a material particular; and

(b) which is so supplied for the purpose of having the Commissioner consent to the matching procedure to which the request relates, commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.

(5) A data user (including a data user first-mentioned in section 32(2)) who contravenes any condition specified in a notice under section 30(2) or 32(1)(b)(i) commits an offence and is liable on conviction to a fine at level 3.

(6) Any person who contravenes section 44(3) or 46(1) commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.

(7) Subject to subsection (8), any relevant data user who contravenes an enforcement notice served on the data user commits an offence and is liable on conviction to a fine at level 5 and to imprisonment for 2 years and, in the case of a continuing offence, to a daily penalty of $1000.

(8) It shall be a defence for a relevant data user charged with an offence under subsection (7) to show that the data user exercised all due diligence to comply with the enforcement notice concerned.

(9) Any person who -

(a) without lawful excuse, obstructs, hinders or resists the Commissioner or any other person in the performance of his functions or the exercise of his powers under Part VII;

(b) without lawful excuse, fails to comply with any lawful requirement of the Commissioner or any other person under that Part; or

(c) makes a statement which he knows to be false or does not believe to be true, or otherwise knowingly misleads the Commissioner or any other person in the performance of his functions or the exercise of his powers under that Part, commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.

(10) A data user who, without reasonable excuse, contravenes any requirement under this Ordinance (other than a contravention of a data protection principle) for which no other penalty is specified in this section commits an offence and is liable on conviction to a fine at level 3.

(Enacted 1995)

**Chapter: 486 PERSONAL DATA (PRIVACY) ORDINANCE**
**Section: 65 Liability of employers and principals**

(1) Any act done or practice engaged in by a person in the course of his employment shall be treated for the purposes of this Ordinance as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval.

(2) Any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of this Ordinance as done or engaged in by that other person as well as by him.

(3) In proceedings brought under this Ordinance against any person in respect of an act or practice alleged to have been done or engaged in, as the case may be, by an employee of his it shall be a defence for that person to prove that he took such steps as were practicable to prevent the employee from doing that act or engaging in that practice, or from doing or engaging in, in the course of his employment, acts or practices, as the case may be, of that description.

(4) For the avoidance of doubt, it is hereby declared that this section shall not apply for the purposes of any criminal proceedings.

(Enacted 1995)

**Chapter: 486 PERSONAL DATA (PRIVACY) ORDINANCE**
**Section: 66 Compensation**

(1) Subject to subsection (4), an individual who suffers damage by reason of a contravention-

(a) of a requirement under this Ordinance;

(b) by a data user; and

(c) which relates, whether in whole or in part, to personal data of which that individual is the data subject, shall be entitled to compensation from that data user for that damage.

(2) For the avoidance of doubt, it is hereby declared that damage referred to in sub-section (1) may be or include injury to feelings.

(3) In any proceedings brought against any person by virtue of this section it shall be a defence to show that-

(a) he had taken such care as in all the circumstances was reasonably required to avoid the contravention concerned; or

(b) in any case where the contravention concerned occurred because the personal data concerned were inaccurate, the data accurately record data received or obtained by the data user concerned from the data subject or a third party.

(4) Where an individual suffers damage referred to in subsection (1) by reason of a contravention referred to in that subsection which occurred because the personal data concerned were inaccurate, then no compensation shall be payable under that subsection in respect of so much of that damage that has occurred at any time before the expiration of 1 year immediately following the day on which this section commences.

(Enacted 1995)

## KEY TERMS

| Term | Description |
|---|---|
| Electronic Health Record (eHR) | A record in electronic format containing health-related data of an individual. |
| eHR Sharing System | A Government-owned electronic platform for healthcare providers to upload and access individuals' health-related data. |
| Patient-under-care principle | Healthcare providers may only access the health data of only patients who have given their consent and for whom they are delivering care. |
| Need-to-know principle | Healthcare providers may only access to those health data that are necessary for the delivery of care for the patients. |
| eHR sharable scope | Pre-defined scope of health data which will be accessible by other healthcare providers over the eHR Sharing System. Only data necessary and beneficial for the continuity of healthcare will be included. |
| Person Master Index (PMI) and PMI data | Through primarily the use of Hong Kong Identity Card with system data validation, an index centrally maintained by the eHR Sharing System to uniquely identify individual patients. PMI data may include the Chinese and English names of the patient, his/her identity document number, date of birth, sex, address, mobile phone number, etc. |
| Role-based access control | Different level of access to the contents of health data in the eHR Sharing System for healthcare professionals with different roles. |
| Privacy Impact Assessment | A systematic risk assessment process that evaluates a proposal in terms of its impact upon personal data privacy with the objective of avoiding or minimising adverse impacts. |

# ABBREVIATIONS

| | |
|---|---|
| CMS | Clinical management system |
| COP | Code of Practice |
| DAR | Data access request |
| DCR | Data correction request |
| DH | Department of Health |
| DPP | Data Protection Principle |
| eHR | Electronic Health Record |
| eHR Core | eHR core sharing infrastructure |
| EEI | eHR Engagement Initiative |
| eHR-OB | eHR Sharing System operating body |
| eHS | eHealth System |
| eMR/ePR | Electronic medical/electronic patient record |
| FHB | Food and Health Bureau |
| GOPC | General out-patient clinic |
| HA | Hospital Authority |
| HKCTT | Hong Kong Clinical Terminology Table |
| HKID | Hong Kong Identity Card, also known as Smart ID Card |
| HKMA | Hong Kong Medical Association |
| HKMA CMS 3.0 | HKMA Clinic Management System 3.0 |
| HL7 | Health Level 7 |
| ICD-10 | International Classification of Diseases, 10th Revision |
| ICPC2 | International Classification of Primary Care 2 |
| IT | Information technology |
| LegCo | Legislative Council |
| LOINC | Logical Observation Identifiers Names and Codes |
| MIP | Mentally incapacitated person |
| NGO | Non-governmental organisation |
| PCPD | The Office of the Privacy Commissioner for Personal Data |
| PDPO | Personal Data (Privacy) Ordinance (Cap.486) |
| PIA | Privacy impact assessment |
| PMI | Person Master Index |
| PPI-ePR | Public-Private Interface – Electronic Patient Record |
| PPP | Public-Private Partnership |
| SDM | Substitute decision maker |
| SFH | Secretary for Food and Health |
| SNOMED CT | Systematised Nomenclature of Medicine, Clinical Terms |
| SOA | Service oriented architecture |
| Steering Committee | Steering Committee on eHR Sharing |
| The Framework | The Legal, Privacy and Security Framework for eHR Sharing |
| WG | Working Group on Legal, Privacy and Security Issues under the Steering Committee on eHR Sharing |

醫健通
ehealth
香港特別行政區政府 HKSAR GOVT

www.ehealth.gov.hk

Published by the Food and Health Bureau
Printed by the Government Logistics Department
Hong Kong Special Administrative Region Government