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

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.

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