LC Paper No. CB(2)2279/11-12(05)

For Discussion
on 11 June 2012

Legislative Council Panel on Health Services

Report on Public Consultation on the Legal, Privacy and Security Framework for Electronic Health Record Sharing

PURPOSE

This paper briefs Members on the outcome of the public consultation on the Legal, Privacy and Security Framework (the Framework) for Electronic Health Record (eHR) Sharing, and sets out our proposed way forward.

BACKGROUND

2. One of the healthcare reform proposals put forward by the Government in 2008 is the development of a territory-wide eHR Sharing System. The proposed 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 sectors thereby promoting public/private sector collaboration, continuity of care and the quality of healthcare delivery. 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 approved the funding commitment for the first stage of the eHR programme from 2009-10 to 2013-14. On 12 December 2011, we launched a two-month public consultation on the Framework for eHR Sharing. We made a presentation to Members and undertook to revert to this Panel on the outcome of the public consultation.

PUBLIC CONSULTATION

3. We aimed to solicit views from both the stakeholders and the general public during the consultation. We uploaded the consultation

document on eHR Office's website, distributed copies of the document to the public, invited interested organisations to send us views, arranged broadcast of Announcement in the Public Interest on TV and radio, studied the opinions expressed in Home Affairs Bureau's on-line forum and attended meetings/briefing sessions to explain our proposals to stakeholders. We received a total of 111 responses. The key proposals of the Framework and the number of comments received on them are set out at **Annex A**.

RESPONSES FROM PUBLIC CONSULTATION

4. Of the 111 responses, 69 were from individuals and 42 from groups/organisations. A list of these 111 individuals and groups/organizations is at **Annex B**. A summary of the views expressed is at **Annex C**.

ANALYSIS OF VIEWS GATHERED

5. Judging from the responses, the public remains very supportive towards the plan for development of the eHR Sharing System in Hong Kong. We do not see strong objections or reservations in respect of the guiding principles for developing the eHR Sharing System set out in the Framework. There are, however, different views expressed on several issues. The Steering Committee on eHealth Record Sharing (EHRSC) and the Working Group on Legal, Privacy and Security Issues (WG-LPS) have carefully considered and deliberated on the responses received. The analysis below sets out the key areas of concern and the recommendations of the EHRSC and WG-LPS.

Patient Access

(a) Views gathered:

6. Nineteen respondents commented on this issue. The respondents' main concerns are the patient's rights and convenience of access to eHR data. They generally considered that patients should have the right to easily access and download their eHR data. Some of the respondents supported the proposed data access arrangement in the form of "data access request" (DAR). However, some expressed concern about the potential distress or misunderstanding caused to patients if they are allowed to make easy access to their medical data. There are also concerns about the charges imposed on

making DAR.

7. Some respondents were keen to see access to eHR be made even more convenient. They proposed that patients should be allowed to access their eHR through an online portal or via their mobile phones.

(b) Analysis:

8. We respect patients' rights of access to eHR data. We envisage that the fee for DAR will not be high because under the future eHR Sharing System, the administrative cost for generating electronic copies is unlikely to be substantial. As such, imposing a charge which helps to recoup the administrative cost for providing the data should not produce any deterring effect on patients making DAR.

9. Some patients, especially the younger generation, considered that a "Patient's Portal" should be developed and implemented as early as possible for more convenient access to eHR. However, both EHRSC and WG-LPS have expressed concern that there is a need to balance between convenience of access, the risk of misinterpretation of the health data by the patient in the absence of a healthcare provider's professional advice or counselling, and the additional security risk to the eHR Sharing System if access is provided through an open "Patient's Portal" system. We propose to carefully examine the merits and risks of developing the "Patient's Portal" and the case for providing more channels of access in the second stage of the eHR Programme, taking into account relevant overseas experience in launching similar eHR projects.

Sharable scope and exclusion of data

(a) Views gathered:

10. Having considered the pros and cons of providing a "safe deposit box", i.e. an electronic data feature which allows the separate storage of certain patient data with enhanced access control, especially the complexity and the extra cost involved in the design and operation of the eHR system, possible clinical risk, and the need to ensure the completeness of the eHR and the integrity of the eHR Sharing System which is necessary to enhance the quality of healthcare delivery, we did not recommend in the consultation document the inclusion of such a feature in the eHR Sharing System. We subsequently received 23 comments on this issue. Those in favour of providing a "safe

deposit box" were of the view that patients should have the right to choose the data to be shared. They considered that "sensitive data" such as information on psychiatric diseases/mental conditions, hereditary diseases, AIDS and other sexually transmitted diseases should not be easily accessible, which will help protect the patients from discrimination. Patients should be allowed to add additional access control device, encryption or other safeguards for protecting sensitive data, or to exclude sensitive data from eHR entirely.

11. Some respondents further suggested that we should enable patients to move data in and out of the "safe deposit box" anytime. Moreover, by allowing more types of data to be put inside the "safe deposit box", it could help minimize the possible labeling effect. On the other hand, some respondents argued that the additional encryption or exclusion of data should not be allowed in respect of information concerning infectious diseases (e.g. hepatitis, AIDS). They saw the need to protect healthcare professionals and the public from being infected.

12. As an alternative, some suggested that the access to sensitive data might be restricted on a "need-to-know" basis to only relevant healthcare professionals (e.g. psychiatric data could only be seen by psychiatric doctors).

13. There were also respondents who supported the idea of not providing any "safe deposit box" at all. They pointed out that the arrangement of withholding certain key data from the health record of patients would undermine the merit of eHR sharing and adversely affect healthcare quality. Some even remarked that it would be inappropriate to let patients make the decision on what medical data should be shared.

(b) Analysis:

14. As in other countries where eHR sharing systems are being implemented, there are divergent views on the issue of allowing additional access control or exclusion of particular data from the eHR sharable scope. In the local context, the Hospital Authority (HA) currently does not provide any "safe deposit box"-like feature in its Clinical Management System[1]. HA medical records are accessible by healthcare professionals of HA on a "need-to-know" basis. Under our proposed eHR Sharing System, role-based access control will be implemented to ensure that only relevant healthcare

[1] HA has developed its Clinical Management System since 1995 for storing and retrieving HA patient's medical records.

professionals could view records on a "need-to-know" basis. Moreover, all healthcare providers participating in eHR sharing would be required to exercise proper internal access control.

15. In the consultation document we have explained the difficulty for healthcare professionals to determine which particular data should be regarded as sensitive. Apart from the names of disease, other data contained in a medical record (e.g. name of specialists, medications) may also point to a patient's health status. At this stage, we are not aware of any successful overseas examples of operating "safe deposit box" in eHR sharing. Australia plans to enable patients to withhold selected information in their Personally Controlled Electronic Health Record System. However, the system has not yet commenced operation. While acknowledging that some patient groups would wish to have enhanced access control on sensitive health data, the WG-LPS and EHRSC consider it necessary to assess the implication of the exclusion of some data by the patients in the eHR, especially to the integrity of the system and the objective of eHR sharing.

16. Those representing the medical professions at WG-LPS and EHRSC have expressed concern that reliable health records containing essential data are necessary to enable healthcare professionals to exercise better judgment. By enabling the sharing of medical information, the eHR Sharing System would facilitate transfer of health record and hence promote collaboration between public and private healthcare providers. The ultimate goal is to improve the quality and continuity of healthcare services to patients. They felt that hiding of certain health information would undermine the trust between the patient and the healthcare professional. A healthcare professional might not want to take the professional and legal risk of treating a patient who deliberately withholds certain part of his medical history from him.

17. Indeed, the voluntary nature of the eHR Sharing System has already provided flexibility for the patients to control access to their health data. If the patients have genuine concern, they could choose to grant consent only to those healthcare providers that they trust. Only these healthcare providers may then upload data to or view the concerned patients' eHR and a "safe deposit box" would not be required.

18. In view of the complexity of the issue, the Administration considers that it should be further studied with reference to overseas experience. There is flexibility in the eHR Sharing System to incorporate such features in

the future eHR development. We recommend that the study on additional access control for sensitive data should proceed in tandem with the study on "Patient's Portal" for the next stage of the eHR Programme.

eHR of withdrawn/deceased patients

(a) Views gathered:

19. Thirteen submissions commented on the handling of eHR of withdrawn/deceased patients. Respondents generally supported the proposed arrangement of "freezing" the eHR when the patient has withdrawn from the eHR System or passed away. However, there are different views on the appropriate length of the frozen period. While some respondents supported our proposal of "freezing" eHR of withdrawn and deceased patients for three and ten years respectively, some suggested shortening the frozen period for deceased patients to six years. One respondent proposed a uniform seven years retention policy be adopted. The longest frozen period suggested is 15 years for deceased patients.

(b) Analysis:

20. Although some respondents expressed preference for a different retention period, they did not provide detailed arguments to substantiate their recommendation. When formulating our proposal, we have examined the relevant sections in the Limitation Ordinance (Cap. 347). In general, the limitation period for actions related to tort is six years from the date on which the cause of action arises. Where the claimant is a "disabled" person[2], the limitation period can be extended: the action may be brought at any time before the expiration of six years from the date when he/she ceases to be "disabled" or has died, whichever event first occurred. In any case, an action for damages for negligence shall not be brought after the expiration of 15 years from the date on which the negligent act or omission occurred. In other words, the limitation period may vary from six to 15 years depending on the circumstances.

21. On balance, we consider 10 years a reasonable length of period for retaining the eHR of a deceased person. It should provide sufficient time for a claim against negligent act to be made by the estate of the deceased person,

[2] Defined in the Limitation Ordinance (Cap.347) as an infant or a person of unsound mind. An infant is a person who has not attained the age of 18 years as defined in the Interpretation and General Clauses Ordinance (Cap.1).

without having to retain the eHR for an excessively long period. As for participants withdrawing from the eHR System, it is recommended that their health record should be kept for three years, which should be sufficient to cater for possible personal injuries or fatal accident claims and if necessary the data subject may rejoin eHR sharing or request for a copy of the data to enable him to continue to pursue the claims.

eHR Sharing System Operating Body

(a) Views gathered:

22. The consultation document has mentioned some of the functions to be performed by eHR Sharing System operating body (eHR-OB) in running the future eHR Sharing System. Eleven respondents commented on the eHR-OB's governance and operation. Some requested for clarifications on the power and responsibility of the eHR-OB. In particular, some respondents suggested that we should empower the eHR-OB to conduct audits on the relevant electronic record systems of the participating healthcare providers, and to handle medical information of withdrawn/deceased patients. To enhance the transparency and accountability of the eHR-OB, some respondents suggested that key stakeholders (including the medical and information technology sectors) should be engaged in its future governance structure.

23. Some respondents argued that from the public confidence perspective, an independent governing body could better ensure effective implementation and enforcement. Some suggested an independent body should be set up and tasked to investigate complaints and monitor/audit operation of the eHR Sharing System.

(b) Analysis:

24. To ensure compliance, the eHR-OB should be empowered to commission security audits on both the relevant electronic record systems and the internal access control systems of participating healthcare providers. We will draw up relevant security policies and procedures. The audits could be initiated as compliance checks or for investigation of complaints. Regular security audits will also be conducted on the eHR Sharing System to ensure the integrity of the System and its safe and secure operation.

25. On transparency and accountability, we will devise the respective

code of practice for not just the participating healthcare providers, but also the eHR-OB. We will also suitably engage stakeholders of relevant sectors in its governance structure. Appropriate channels for handling complaints will be put in place. The mechanism will be prudently designed to minimise any potential conflict of interest. Depending on the nature of the complaints, they could be handled by appropriate internal or external authorities.

WAY FORWARD

26. We have gathered valuable advice and suggestions in the public consultation exercise. We welcome any further views from Members and would refine the Framework as appropriate. We will commence drafting the eHR legislation, with a view to introducing the bill to the Legislative Council in 2013-2014 and implementing the first stage of the eHR Sharing System by end 2014.

Food and Health Bureau
June 2012

Annex A

Public Consultation
on the Framework for eHR Sharing

Subject	Proposal in the Framework	No. of comments received
(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.	28
(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 the Hospital Authority and Department of Health to access a patient’s eHR should be part and parcel to the enrolment to eHR sharing.	20
(c) Substitute Decision Maker (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.	14
(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.	12
(e) eHR of withdrawn or deceased patients	The eHR data of withdrawn or deceased patients will be kept for 3 years and 10 years respectively before being de-identified.	13
(f) eHR sharable scope	No “safe deposit box” and no exclusion of data.	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 Sharing System operating body (eHR-OB) or the Secretary for Food and Health.	16

Subject	Proposal in the Framework	No. of comments received
(h) Data access and correction	For better protection of the patients' privacy, only subject patient, person with parental responsibilities over minor, and guardian of mentally incapacitated person appointed by Court can make a data access request (DAR) or a data correction request (DCR) to eHR-OB. Any amendments would be marked in tracking mode.	35
(i) Criminal sanctions	A stronger deterrent against unauthorised access to the eHR Sharing System with malicious intent would be introduced through the eHR legislation.	18
(j) Various security measures on eHR data		
i.	Code of practice (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.	21
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.	37
iii.	Data encryption, data validation, proof integrity and origin of eHR data.	26
iv.	Limited downloading of eHR data – Only Person Master Index data and allergy information, which are necessary for clinical record management and decision support, may be downloaded from the eHR Sharing System.	14
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.	24

Annex B

Public Consultation on the Framework for eHR Sharing

List of Respondents

No.	Name
1	(Respondent with no name provided)
2	Wong Yuen Lee
3	astro
4	Cheung Chung Fu Desmond
5	Middle Class Dude
6	QYKL
7	Michelle Li
8	Lawrence J. Lau
9	HK citizen
10	侯平中醫師
11	辰龍客
12	(Respondent requested keeping name and views confidential)
13	PEKY
14	Elderly Commission
15	RANDY KU
16	Hospital Authority
17	Heidi
18	Godfrey
19	Horace
20	Chung Ching May
21	Anita Varshney
22	Poon Shiu Man Henry
23	Chow Wai Yee
24	HW
25	KC Luk
26	(Respondent requested keeping name and views confidential)
27	(Respondent requested keeping name and views confidential)
28	WONG Chan
29	Chan Lim Yue Teresa
30	(Respondent requested keeping name and views confidential)
31	Dr. Eric Lo
32	Szeto, H.K.
33	Chen Chung Nin Rock
34	白金
35	KW

No.	Name
36	(Respondent with no name provided)
37	Dr. S P Chan
38	Dr Anthony KY Lee
39	Helen Chu
40	Joseph Li
41	Pun Kwok Shan
42	Hong Kong Doctors Union
43	LAU Chi Kin, Vincent
44	GS1 Hong Kong
45	Ma Kam Wah Timothy
46	Ma Kam Wah Timothy *(Content different from No. 45)*
47	Forest KC Wong
48	The Pharmaceutical Society of Hong Kong
49	Lily Chan
50	(Respondent requested keeping name and views confidential)
51	施鳴
52	margaret lam
53	eHealth Consortium Limited
54	Digital 21 Strategy Advisory Committee Task Force on e-Government Service Delivery
55	Tom Lam
56	Baker & McKenzie
57	Mok Kwan Ngan Hing Edith
58	(Respondent requested anonymity)
59	cck
60	楊位醒
61	(Respondent requested keeping name and views confidential)
62	Sidney K
63	The Hong Kong Coalition of AIDS Service Organizations
64	東華三院賽馬會復康中心
65	The Hong Kong Institution of Engineers
66	邱榮光博士
67	The Institution of Engineering and Technology Hong Kong
68	Chiropractors Council Hong Kong
69	Caring Hong Kong
70	Fu Hong Society
71	Mr. Kiwi Chan
72	Senior Citizen Home Safety Association
73	CHAN HON FUN
74	Internet Professional Association
75	Alliance for Patients' Mutual Help Organizations and 43 Patient Groups

No.	Name
76	HL7 Hong Kong Limited
77	Association of Hong Kong Nursing Staff
78	Mr. Cheung Yee Tak Derek (Respondent requested keeping views confidential)
79	The Law Society of Hong Kong
80	Alliance for Renal Patients Mutual Help Association
81	Business and Professionals Federation of Hong Kong
82	The Hong Kong Federation of Insurers
83	一名市民
84	The Office of the Privacy Commissioner for Personal Data
85	Hong Kong Computer Society
86	Hong Kong Dental Association
87	NG Chuck-nam
88	Students from Master of Science in Health Informatics programme of the Hong Kong Polytechnic University
89	Kelvin
90	ITVoice 2012 Team
91	PCCW Solutions
92	Clifford Tse
93	The Professional Commons
94	Internet Society Hong Kong
95	Hong Kong Information Technology Federation
96	Civic Party
97	香港復康聯會
98	推動精神健康政策聯席
99	The Hong Kong Medical Association
100	Hong Kong Bar Association
101	Information Systems Audit and Control Association China Hong Kong Chapter
102	Hong Kong Academy of Medicine
103	The Practising Pharmacists Association of Hong Kong
104	Professor John Bacon-Shone
105	iy chi
106	Town Health Medical & Dental Services Limited
107	Consumer Council
108	(Respondent requested keeping name and views confidential)
109	(Respondent requested keeping name and views confidential)
110	(Respondent requested keeping name and views confidential)
111	a seed of

Public Consultation on the Framework for eHR Sharing

Summary of Views

Issue	Proposal	Summary of views *(related number of response)*
(a) Voluntary participation	Patients and healthcare providers would participate in electronic health record (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.	• Support voluntary participation by patients and healthcare providers as proposed (20). • Against voluntary participation by healthcare providers and asked if it should be mandatory for healthcare providers to join eHR in future (3). • Support "opt-out" instead of "opt-in" (4). • Other comments: - Sufficient information should be provided to patient through the Patient Information Notice. - Existing arrangement on sharing health-related data should still be available to those who choose not to join eHR.
(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 Hospital Authority (HA) and the Department of Health (DH) to access a patient's eHR should be part and parcel to the enrolment to eHR sharing.	• Consent should be "open-ended until revocation" (5 support & 2 against). • "One-year" consent (5 support & 3 against). • Prefer time restricted or one-off consent (3). • Other comments : - Suggest "deemed renewal" consent: renewal letter will be sent to the patient. If the patient does not object to the arrangement, consent is deemed to be renewed. - Patients should be informed of the difference between "one year" and "open-ended" consent. - Process to obtain consent must be simple and easy to trigger, in particular during emergency. - Consent must be clearly documented. Express and informed consent should

Issue	Proposal	Summary of views *(related number of response)*
		be included in Patient Information Notice. Suggest mandatory verbal explanation by healthcare providers followed by patient's signature acknowledgement. - Question why consent to HA & DH are "open-ended" and hence treatment different from other healthcare providers. - Agree that consent to the HA/ DH should be part and parcel of patient's enrolment to eHR sharing. - Patient should be informed that by virtue of enrolment by a patient, the HA and/or DH have an automatic right to upload all patient's information. - Suggest allowing patients to switch between the two types of consent. - For referrals, patients should be provided with information about the identities of the recipients before data transfer. Suggest obtaining consent on a case-by-case basis.
(c) Substituted Decision Maker (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.	• Support SDM proposal (5). • Support that minor should be under 16 (2). • Propose consent age/minor's age should be 18 (2). • Other comments: - Process for healthcare providers to be SDM should be simple, efficient and effective. - Co-habitant can act as SDM if the patient has no immediate family members. - Guidelines should be given for elderly home healthcare professionals to ensure validity of the consent they give on behalf of the patients. - SDMs for mentally incapacitated persons (MIPs) could include parents, guardian, immediate family members and healthcare providers of the MIPs. - Ask if there is any mechanism to handle situations where immediate family members have different views on whether the patient should join eHR.

Issue	**Proposal**	**Summary of views *(related number of response)***
(d) Exemption	Under exceptional circumstances (e.g. delivery of emergency care) eHR data may be accessed by healthcare providers without the subject patient's consent.	• Support exemption proposal (6). • Other comments: - Guidelines should be developed around what constituted an emergency situation. - Proper mechanism and independent party to see if access is justified. - Patient should be informed of the exemptions arrangement when he/she joins eHR.
(e) eHR of withdrawn or deceased patients	The eHR data of withdrawn or deceased patients will be kept for 3 years and 10 years respectively before being de-identified.	• For withdrawn patients' records - to be frozen for 3 years (5 support). • Other comments: - Suggested uniform frozen period of 7 years. - Various suggestions for deceased patient's data to be frozen ranging from 6 or 15 years. - Suggest patient to be consulted on the duration of frozen period.
(f) eHR sharable scope	No "safe deposit box" and no exclusion.	• Support no "safe deposit box": (5). • Suggest having "safe deposit box" or patient has the right to choose data: (18). • Other comments : - Should have save deposit box built in the system for future use. - Should include medical records before implementation of eHR. - Propose variations to eHR sharable scope to include: contagious disease such as Hepatitis, AIDS so as to protect healthcare providers, nursing records, radiological images, and multimedia data health records. - Against unscreened data to be provided to patients which can cause misunderstanding. - Suggest allowing patients to have the right to move highly sensitive/ private data such as hereditary diseases, sexually transmitted diseases and mental diseases in and out of the safe deposit box anytime by themselves.

Issue	Proposal	Summary of views *(related number of response)*
		- Provided a safe deposit box is available, support the proposal of not allowing exclusion of eHR data from sharing.
(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 Sharing System operating body (eHR-OB) or the Secretary for Food and Health (SFH).	• Support secondary use as proposed (5). • Support secondary use on de-identified data only (2). • Other comments : - Secondary use: trend analysis pattern for laboratory results, clinical research on drugs or drugs safety. - Should not be sold to third parties. - Data in eHR would be a good resource for future policy formulation and services planning. - Since eHR participation is on voluntary basis, eHR data is unlikely to be complete record and is unreliable or irrelevant for secondary use. - Recommended de-indentified data to be retained for research and statistics purposes. - Ask about the criteria for allowing data to be used for secondary purposes. - There are not enough patient representatives from the public sector at the research board and the board does not seem to have privacy professional. - Secondary use for patient identifiable data must be approved by the Office of the Privacy Commissioner for Personal Data in addition to SFH on recommendation by a research board. - Patients should be informed of the possibility of secondary use in the Patient Information Notice.
(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 data access	• Support DAR (7). • Support DCR (5). • Opine that patients should have right to access their eHR (6). • Anticipate to access patient's record online or through patient's portal (7). • Other comments:

Issue	Proposal	Summary of views *(related number of response)*
	request (DAR) or a data correction request (DCR) to eHR-OB. Any amendments would be marked in tracking mode.	- Patients should be the data owner of eHR. - Original data cannot be overwritten may result in storage of unnecessary information contrary to Data Protection Principle (DPP) 2 and cause confusion. Legislation may need specific exemption to DPP2. - Clarification of the extent of healthcare provider's liability if data is inputted incorrectly. - Do not support mobile access to patient's eHR but there is also suggestion for allowing mobile access of patient's data by healthcare professional. - Question why not allowing authorised third party to have DAR. Inconsistent with general access right under Personal Data (Privacy) Ordinance (PDPO). - To allow healthcare providers to access the frozen data of deceased patients should there be medical legal claims involved. - 3rd party e.g. lawyers, insurance companies or overseas doctors to be allowed to make DAR. - eHR-OB should ensure healthcare providers respond to a DCR within a certain period of time. - Fee for DAR should be directly related and necessary, and non-excessive. - Has reservation on the potential service charge on patients, especially the lower income citizens. - Worried about the workload of doctors in public hospitals.
(i) Criminal sanctions	A stronger deterrent against unauthorised access to the eHR Sharing System with malicious intent would be introduced through the eHR legislation.	• Support criminal sanction (8). • Other comments: - Prefer a new legislation for this. - Suggest misconducts leading to sanction: sharing of login account, misused/leaked patients' data for other purposes and negligence or recklessness.

Issue	Proposal	Summary of views *(related number of response)*
		- Suggest other types of sanction: stringent punishment/severe penalty, monetary sanction, civil sanction for breaches with a lower threshold of culpability and suspend licence of healthcare providers in case of serious/repetitive breaches. - Penalty should commensurate with penalty level under PDPO and Personal Data (Privacy) (Amendment) Bill 2011.
(j) **Various security measures on eHR data**		
i. Code of practice (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.	• Support COP (7). • Other comments: - Should clarify the legal liability/effect of COP and consequences of non-compliance of COP. - Proposed items to be included in COP: login details should not be disclosed to other party, doctor must read eHR if available, stringent guidelines to stop the abuse of using and accessing eHR, set out the audit requirements in COP. - Suggest having a compliance officer post in each hospital and clinic. - There should be COP on governance of eHR-OB and eHR Sharing System. - COP should be developed in consultation with patient groups. - More appropriate for Medical Council to study, screen and approve COP. - To extend control beyond downloading of eHR. - Standard guidelines should be drawn up for crucial practice and all healthcare providers should follow them.
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	• Support the proposed role-based access control (9). • Other comments: - Support authentication of patients & healthcare providers. - Different suggestions on healthcare providers to be included: medication staff & medical analysts, dentists, optometrists, psychiatrists, research nurses and

Issue	Proposal	Summary of views *(related number of response)*
	implemented.	assistants, registered nurses or Nursing-Team-in-Charge of NGO or authorised healthcare worker with different access rights, healthcare professionals in private hospitals, clinics, elderly homes and other residential services, doctors only, nursing staff in residential care home for the disabled, pharmacists, laboratory technologists, dietitians and Chinese medicine practitioners. - Object to include insurance companies. - Sharing with public hospitals and clinics only. - Nurses should be allowed to upload prescription and access eHR. - Authentication: use patient's ID no. and finger print, anticipate more patient identification options. - Allow patients to customise access level for different healthcare providers. - Consider separate consent for uploading and consent for accessing eHR. - Only healthcare providers of particular discipline to access the specific scope of data, e.g. psychiatric records only opened to psychiatrists. - To make known to the public the access right of different healthcare providers. - eHR-OB to set standard "role-based access control" to ensure uniform practice of healthcare providers.
iii. Data encryption, data validation, proof of integrity and origin of eHR data		• Support the proposal (3). • Other comments: - Emphasise the importance of data/system security, encryption and prevention of leakage and misuse of data. - Accuracy and reliability of information keyed into the system should be ensured. - Certification is required to ensure that private healthcare providers' systems are well designed to control access to eHR and safeguard patient's data.

Issue	Proposal	Summary of views *(related number of response)*
		Both technical and procedural compliance of electronic medical/ electronic patient record (eMR/ePR) systems should be renewed regularly. - Authentication of healthcare providers by digital cert/signature. - The system should guard against double login. - No share use account for healthcare providers.
iv. Limited downloading of eHR data	Only Person Master Index (PMI) data and allergy information, which are necessary for clinical record management and decision support, may be downloaded from the eHR Sharing System.	• Support the proposal (7). • Other comments: - Only allow part of PMI to be downloaded, e.g. HKID card no. A123XXX, address: Tsuen Wan - Need to consider other preventative measures and monitor inappropriate access/leakage of eHR data. - To allow printout of prescription information. - Information viewable by doctors should not be kept as a local copy or used illegally without patient's prior consent. - Restricted download or disabling data download function cannot completely avoid data leakage, and it can hinder the usability of eHR.
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.	• Support access notification by Short Message Service (SMS) (5). • Other comments: - Emphasise the need to protect privacy and avoid misuse or abuse of information in eHR. - Consider to allow patients to authorise other person to enquire about the access history. - More focus on education on potential legal implication of breaching data privacy. - Ask what sanctions will be imposed if the subject patient is not notified of the breach.

Issue	Proposal	Summary of views *(related number of response)*
		- There should be other access notification options for elderly, people with no mobile phone, infrequent mobile phone users or people who are not familiar with using SMS, other than SMS and e-mails. - Incidents of security or privacy breaches should be made known to the public. - Consider only to send access notification for suspected unauthorised access. - Suggest mandatory reporting mechanism for any data security breach and potential data security breach to Privacy Commission or other Government agencies. - Suggest mandatory logging for access by users for tracking and potential investigation of abuse, breach, etc. - Further legislation on the data users on mandatory reporting of data breach. - Certification/audit should subject to independent assessment.
(k) **Other issues**		
i. General concept and approach of eHR sharing		• Support (50), against (2). • Other comments: - Only support eHR sharing in public sector, but object to sharing with private sector (1).
ii. eHR specific legislation and legal issues		• Support (6). • Ask whether the role of Privacy Commissioner will be extended to privacy protection compliance under eHR legislation. • Statutory standard of care for handling and storage of eHR data to be imposed on healthcare providers and DH and HA. • Ask who will be liable in the event of system error, data leakage, data loss or system hacking. Recommend that this issue be addressed in eHR legislation and ask whether there is any recourse to individuals suffering from such loss. • New legislation should specify that it does not override PDPO, add additional

Issue	**Proposal**	**Summary of views *(related number of response)***
		protection. • Other comments: - Amendment to PDPO might be required. - Should have indication on the proposed interface between PDPO and the new eHR legislation, avoid double penalties. - Including penalties provisions for the breach of serious issues in COP/ guidelines. - Suggest imposing different kinds of punishment for “inadvertent omissions and errors” of different nature that caused serious harm to the patient.
iii. eHR-OB governance & related issues		• eHR-OB should be the empowered authority of performing “security audits on the eMR/ePR systems” and internal access control of healthcare providers. • eHR-OB shall be an independent organisation and act as a custodian of the eHR Sharing System, and to provide the day-to-day operation as well as to take on complaints/issues related to the eHR Sharing System. • Recommend setting up of an independent arbitration organisation to consider punishment and compensation against misuse/ leakage of patients’ data • Complaints to be reviewed by an independent committee. • Concerned about governance, transparency and accountability of eHR-OB. • Independent party to monitor and audit the operation of eHR Sharing System and provide regular report to public. • Support eHR-OB be empowered to issue and maintain a regularly updated COP. • An independent eHR Data Privacy Commissioner to protect patients’ interest.
iv. Security and technical issues		• Data should be stored in a privately managed server, but not a cloud platform. • Recommend a simple and standard setting for software component in order to promote diversity or adapted through different software developers.

Issue	Proposal	Summary of views *(related number of response)*
		• Suggested not building a centralised system. Instead, portable smart card should be used for patients to store medical records. • System design should adopt international standard. • Strengthening system security and avoiding hackers intrusion.
v. Miscellaneous		• Propose that the scheme should be valid for HKID holders and not only HK permanent residents. • If patients have medical examinations or operations overseas, input of such information into the system would be required. • Concern about the impact of the eHR Sharing System on purchasing and claiming of medical insurance. • Should give initial support or incentive to healthcare providers for the initial setup and education and continuing technical support. • Financial and technical support to institutions to transform their existing records to a standard electronic format. • Business Continuity Plan should be prepared to ensure that services to patients and medical practitioners are not affected during down time of the system. • Private doctors are concerned that the records may be taken out of context and used as evidence against them. • Consultation with IT professional during system development is required. • Patient Information Notice should be easy to understand. A clear statement of commitment for all participants, including their respective duties and obligations should be included.