# Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals)

The Electronic Health Record Sharing System Ordinance[1] came into operation on 2 December 2015. It provides a legal basis for the collection, sharing, use and safe keeping of patients' health data under the Electronic Health Record Sharing System ("**System**"). The System is an information infrastructure platform for healthcare providers (including doctors and other healthcare professionals) in both the public and private sectors to, with the consent of a patient, access and share the patient's health record in the System for healthcare-related purposes.

The System will commence operation in the first quarter of 2016. Healthcare providers may visit the website of the System (www.ehealth.gov.hk) for more details.

## The Relationship between the Personal Data (Privacy) Ordinance and the System

Patients' health records in the System amount to personal data, which is protected under the Personal Data (Privacy) Ordinance[2]. Healthcare providers and the Commissioner for the Electronic Health Record, as the data users, should act in accordance with the requirements under the Electronic Health Record Sharing System Ordinance as well as the Personal Data (Privacy) Ordinance (including the Six Data Protection Principles) when handling patients' health records in the System.

The functions and powers of the Privacy Commissioner for Personal Data, Hong Kong under the Personal Data (Privacy) Ordinance in relation to personal data in the System include:

- handling complaints of suspected breaches of the Personal Data (Privacy) Ordinance[3] and initiating investigation if necessary;

1 Chapter 625 of the Laws of Hong Kong
2 Chapter 486 of the Laws of Hong Kong
3 Please refer to the Complaint Handling Policy issued by the Office of the Privacy Commissioner for Personal Data, Hong Kong ("**PCPD**")

- carrying out an inspection of the System in respect of its handling of personal data;
- providing guidance on personal data privacy in relation to the System to healthcare providers and citizens; and
- handling any data breach notification in relation to the System.

The Commissioner for the Electronic Health Record has stated in the Code of Practice and Conditions of Registration for Healthcare Providers the requirements on protection of personal data in detail. Before registering with the System, healthcare providers should read relevant provisions carefully. When exercising his functions and powers under the Personal Data (Privacy) Ordinance, the Privacy Commissioner for Personal Data will also take into account the Code of Practice issued by the Commissioner for the Electronic Health Record, in addition to the provisions of the Electronic Health Record Sharing System Ordinance.

## Points to Note for Healthcare Providers and Healthcare Professionals

**1. Patients' participation and giving of sharing consent**

1.1 Health records are sensitive personal data. Healthcare providers should patiently explain the operation of the System to patients in detail to ensure that patients understand the implication of sharing health records on their personal data privacy.

1.2 Healthcare providers must ensure that their staff will remind patients, before giving the joining consent[4] and/or sharing consent[5], to read carefully the "Participant Information Notice" issued by the Commissioner for the Electronic Health Record about the details of the System[6].

1.3 Participation in the System is **voluntary**. A patient may withdraw from the System and revoke his sharing consent given to any healthcare providers[7] at any time. When patients express the above intention, healthcare providers should explain to them in detail the impact of such decision to the healthcare service received and how to make the request to the Commissioner for the Electronic Health Record. From the perspective of personal data privacy protection, even before the withdrawal from the System or the revocation of sharing consent becomes effective, healthcare providers should respect patients' will as much as possible without affecting the related healthcare service.

**2. Access to electronic health record ("eHR") on a "need-to-know" principle**

2.1 **Healthcare providers** must take reasonable steps to ensure that healthcare professionals may have access to only health records relevant to the healthcare service they provide on a "**need-to-know**" principle. For example:

- Set adequate but not excessive access right to the data in the System in accordance with the function and clinical need of various healthcare professionals;

4 Joining consent = Patients agree to let the System store their personal identification and health data from participating healthcare providers who have obtained their consent. Patients are taken to have given a sharing consent (see note 5) to the Hospital Authority and to the Department of Health.

5 Sharing consent = Patients agree to let a particular healthcare provider view and upload their health records.

6 Including the background of the System, what are and how to give joining consent and sharing consent, the sharable scope and use of health data, registration and withdrawal procedures of the System, procedures for revocation of sharing consent, etc.

7 Except the Hospital Authority and the Department of Health

- Incorporate the requirement of keeping patient's information confidential in staff manual or code of practice. Timely review the staff's access right to the data in the System, and cancel that of departing staff as soon as possible.

2.2 **Healthcare professionals** must, despite having already been authorised by healthcare providers to access eHR, exercise professional judgment to determine what exact data is necessary to be accessed for reference as actually needed in the provision of healthcare service.

## 3. Data accuracy

Healthcare providers should ensure that the eHR provided to the System by them are accurate and comply with the sharing requirements[8].

## 4. Data security

4.1 Healthcare providers shall adopt all **reasonably practicable** steps to protect the personal data in the System. For example:

- Ensure that when authorised staff log into the System, eHR shown on the computer screen will not be seen by unrelated third parties (e.g. consider the direction of the screen and/or use privacy filters);
- Conduct risk assessment for devices and procedures if patients' health records in the System are accessed through notebook computer under specific procedures at non-registered locations for provision of healthcare service (e.g. consultation at patients' home);
- Keep the eHR downloaded or printed from the System[9] (in paper form or otherwise) safely. Guidelines on the use of portable storage devices[10] should be formulated to avoid leakage of personal data;
- Adopt appropriate measures to ensure that healthcare providers' data systems are adequately safeguarded and properly functioned to avoid jeopardising the eHR in the System.

4.2 If there is data breach of the System, healthcare providers should notify the Commissioner for the Electronic Health Record and the Privacy Commissioner for Personal Data[11] as soon as possible.

## 5. Direct marketing

For protection of the vast amount of personal data in the System, healthcare providers must note that using eHR **in the System** in direct marketing is a criminal offence under the Electronic Health Record Sharing System Ordinance. On the other hand, if healthcare providers intend to use the personal data **in their local systems** in direct marketing, they should comply with the requirements under Part 6A of the Personal Data (Privacy) Ordinance[12]; otherwise they also commit a criminal offence.

8 Only data necessary and beneficial for the continuity of healthcare would be included in the scope of eHR sharing: (i) personal identification and demographic data; (ii) clinical note summary; (iii) referral between providers; (iv) adverse reactions and allergies; (v) birth and immunisation records; (vi) other investigation results; (vii) laboratory and radiology results; (viii) diagnosis, procedures and medication; and (ix) summary of episodes and encounters with healthcare providers. (The concerned authority may from time to time review or update the eHR sharable scope. Latest eHR sharable scope and details will be announced at the website of the System (www.ehealth.gov.hk)). Data that fall outside the eHR sharable scope, such as billing and insurance plan information, will not be uploaded, stored and shared through the System.

9 Only patient index data and allergy information can be downloaded from the System to local systems of healthcare providers.

10 Please refer to the "Guidance on the Use of Portable Storage Devices" issued by the PCPD.

11 Please refer to the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the PCPD.

12 Please refer to the "New Guidance on Direct Marketing" issued by the PCPD.

## 6. Personal data privacy policy

Healthcare providers should review their existing personal data privacy policies and make amendments accordingly in order to state their arrangement on the handling of uploading patients' data from their own local system to the System. Such amendments should be properly indicated to patients.

## 7. Data access requests / Data correction requests

7.1 As a healthcare provider is not entitled to provide a patient with eHR uploaded to the System by other healthcare providers, when a patient's data access request for thorough access to his personal data in eHR **in the System** is received, healthcare providers should advise the patient to exercise his data access right under the Personal Data (Privacy) Ordinance by making a data access request to the Commissioner for the Electronic Health Record. Healthcare providers should reply to the patient in writing within 40 days as required under the Personal Data (Privacy) Ordinance[13]. Please note that a healthcare provider should ascertain the target and scope of the request. If a patient makes a data access request to an individual healthcare provider for accessing his personal data in the healthcare provider's **local system**, the healthcare provider should comply with his request in accordance with the requirements under the Personal Data (Privacy) Ordinance[14].

7.2 When a patient's request for correcting his personal data in the System is received, the Commissioner for the Electronic Health Record should, if necessary, make enquiries with the individual healthcare provider concerned about the accuracy of the data as soon as possible. When the healthcare provider is satisfied that the data is inaccurate, it should correct the data immediately and inform the Commissioner for the Electronic Health Record accordingly. Similarly, if a patient makes a data correction request to an individual healthcare provider, the healthcare provider should comply with his request in accordance with the requirements under the Personal Data (Privacy) Ordinance[15].

7.3 Healthcare providers should designate staff to handle data access or data correction requests, and provide proper training and guidelines to the staff on the requirements of the Personal Data (Privacy) Ordinance.

## 8. Complaints

8.1 It is within the jurisdiction of the Office of the Privacy Commissioner for Personal Data, Hong Kong ("**PCPD**") to handle complaints relating to personal data in the System and possible contravention of the Personal Data (Privacy) Ordinance. Upon receipt of such complaints (irrespective of whether it is lodged with the PCPD directly or referred by the Commissioner for the Electronic Health Record), the PCPD will follow them up according to its Complaint Handling Policy.

8.2 To safeguard patients' health records in the System, the Electronic Health Record Sharing System Ordinance has introduced offences relating to accessing, damaging or modifying data in the System. As patients' health records in the System are personal data, a healthcare provider who commits the above offences may also contravene the Data Protection Principles and/or provisions of the Personal Data (Privacy) Ordinance. When such a complaint is received by the Privacy Commissioner for Personal Data and/or the Commissioner for the Electronic Health Record, who opines that an offence may have been committed, under either or both Ordinances, the complaint would be referred to the Police for criminal investigation.

13 Please refer to the Guidance Note on "Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users" issued by the PCPD.

14 See note 13

15 Please refer to the "Guidance on the Proper Handling of Data Correction Request by Data Users" issued by the PCPD.

## Action List for Healthcare Providers before Joining the System for Protection of Personal Data Privacy

As a good practice, healthcare providers should review if adequate measures are adopted to safeguard personal data privacy before joining the System, including:

- ✓ formulate/amend Personal Information Collection Statement
- ✓ formulate/amend Personal Data Privacy Policy
- ✓ set up and test basic facilities (including hardware and software), and conduct risk assessment for devices and procedures
- ✓ provide training to staff on the operation and operating procedure of the System, and formulate relevant codes or guidelines
- ✓ formulate policy on the handling of data access and data correction requests
- ✓ develop procedures for handling complaints related to the System and the mechanism for notifying the Commissioner for the Electronic Health Record
- ✓ set up the mechanism for the handling and notification of data breach of the System

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong
PCPD.org.hk

**Enquiry Hotline :** **(852) 2827 2827**
**Fax :** **(852) 2877 7026**
**Address :** **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
**Email :** **enquiry@pcpd.org.hk**



**Disclaimer**

The information provided in this publication is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (the "Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data (the "Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions provided will not affect the functions and power conferred upon the Commissioner under the Ordinance.

First published in February 2016