Protecting Personal Data
Respecting Patients' Privacy

Stephen Kai-yi Wong
Privacy Commissioner for Personal Data, Hong Kong
Nowadays, leaving a digital footprint is inevitable
Personal Data (Privacy) Ordinance
Chapter 486

• Personal Data (Privacy) Ordinance came into effect on 20 December 1996

• Gazette of the Personal Data (Privacy) (Amendment) Ordinance was published on 6 July 2012. All amendments came into force

• Protecting the privacy right of a “data subject” in respect of “personal data”, but general privacy issues are not protected

• Governs all “data user”
Six Data Protection Principles

• Form the base of the Ordinance

• Data users must comply with the six data protection principles in the collection, holding, accuracy, retention period, security, privacy policy and access to and correction of personal data
Six Data Protection Principles
Collection of Personal Data by Unfair means

• A private doctor recorded the conversations between himself and his patients without the patients’ knowledge

• Contravention of DPP1

• The doctor undertook to cease the act of recording and confirmed that all the audio records had been deleted
Personal Information Collection Statement

• To comply with DPP1, hospitals or clinics should provide patients with a “Personal Information Collection Statement” (PICS) setting out the purpose of collection, the classes of persons to whom the data may be transferred, the consequence if patients fail to provide the data as well as their rights to request access to and correction of their personal data.

• To minimise miscommunication, hospitals or clinics may consider including its PICS at the registration form or display it prominently in the waiting room.
• This Guidance Note serves as a general reference for data users when preparing Personal Information Collection Statement (“PICS”) and Privacy Policy Statement (“PPS”)
• Both PICS and PPS are important tools used respectively for complying with DPP1 and DPP5

Accuracy of Medical Opinions

• The Complainant was diagnosed as having “serious psychosis” by a psychiatry clinic of the Hospital Authority (“HA”), and he later sought consultation at a private clinic and was diagnosed as having “anxiety disorder”. He then lodged a complaint with the PCPD against the HA for holding inaccurate medical records about him.

• No contravention of DPP2

• According to the AAB, medical opinions about judgment of the mental condition of a data subject were the professional judgment of the doctor, and its accuracy was not within the jurisdiction of the Ordinance or the PCPD.
Duration of Retention of Medical Records

• A patient requested his doctor to destroy all his personal data and medical records after he had decided to quit consultation at the clinic.

• DPP2 and section 26 of the Ordinance do not specify the duration of retention of personal data, but stipulate that the data is not kept longer than is necessary for the fulfillment of the purpose for which the data is or is to be used. After the retention period, all practical steps shall be taken to delete the data.

• Duration of retention depends on the retention purpose (e.g. handling of complaints or potential litigation, keeping tax records) and the need to comply with legal requirements.
Improper Use of Patients’ Data

• The Complainant had attended consultations of a resident doctor of a hospital. Later, the Complainant received a call from the doctor and was told that the doctor had resigned and opened a clinic. The doctor checked the Complainant’s address for sending him the new name card.

• The subsequent use of the Complainant’s personal data by the doctor was not directly related to the original purpose of collection of the data (i.e. handling matters relating to diagnosis and treatment for the Complainant). As he had not obtained the patient’s prescribed consent and there was no applicable exemption under the Ordinance, he had contravened DPP3.
Improper Use of Patients’ Data (Con’t)

• The doctor destroyed the personal data of the Complainant and the patients of the hospital, and undertook in writing that he would not so use patients’ personal data in future.
Exemption

- After work injury, the Complainant, a technician of a public transport institution, was referred to psychological treatment during which the Complainant had told the psychologist and counsellor of a service association more than once that he wanted to blow up the public transport facilities of the institution (“the Data”). After consideration and discussion with the psychologist, the association informed the institution of the Data.

- The PCPD considers that blowing up public transport facilities is unlawful or seriously improper conduct under section 58(1)(d) of the Ordinance. The association informed the institution of the Data for the prevention of the above conduct. Under the circumstances, the Data should be exempt from the requirement.
Exemption (Con’t)

• Moreover, the Data was also the personal data relating to the physical or mental health of the technician under section 59 of the Ordinance. If the association could not disclose the Data without the consent of the technician, it would be likely to cause serious harm to the physical or mental health of the technician. Under the circumstances, the Data should also be exempt from the requirement
Failing to Safeguard Patients’ Data

• Case 1: A clinic had made a mistake when using recycle papers. Appointment slips were printed on a paper with 23 patients’ data (including name, partial ID card number, sex and age) on the back.

• Having not taken practical steps to safeguard patients’ personal data, the clinic contravened DPP4.

• The clinic made apologies to the patients affected and issued a letter to the staff concerned reminding them of the duty to protect patients’ data. Measures, including using color papers to print records containing patients’ data, were taken to avoid recurrence of similar incidents.
Failing to Safeguard Patients’ Data (Con’t)

- Case 2: A medical group had mistakenly attached the medical checkup report of a patient to the checkup report of a third party.
- Having not taken practical steps to safeguard patients’ personal data, the group contravened DPP4.
- The group had amended its procedures for handling clients’ checkup reports to ensure that the reports would not contain third parties’ personal data. The PCPD also issued a letter to the group reminding it to handle clients’ checkup reports prudently.
Non-compliance with Data Access Request ("DAR")

• The Complainant made a DAR to a hospital requesting for his medical records and complaint records, but the hospital provided all the data after more than 200 days.

• The hospital had not provided the data within the statutory 40-day time limit, but there was no applicable exemption under the Ordinance. Moreover, the hospital had not informed the Complainant of the situation and the reasons in writing within 40 days, and did not comply with the request as soon as practicable after the expiration of that period. It had contravened section 19 of the Ordinance.

• An Enforcement Notice was served on the hospital directing it to amend the policy and procedures for handling DAR.
Charging Excessive Fee for Compliance with DAR

• After receiving treatment from a dentist, the Complainant made a DAR to the dentist requesting for copies of his X-ray films and medical records. The dentist charged a fee of $10,000
• Investigation revealed that the dentist calculated the cost for locating the data by his hourly salary
• Considering that the fee charged by the dentist was excessive and section 28 of the Ordinance was contravened, the PCPD served an Enforcement Notice on the dentist. As a result, the cost was lowered to $1,260
Offences

• Contravention of a DAR offence, the PCPD may transfer the case to the Police for criminal investigation. The maximum penalty is a fine of $10,000 and 6 months’ imprisonment. A doctor was convicted for failing to comply with a data access request and was fined $1,000

• Contravention of DPP is not an offence. The Commissioner may serve an enforcement notice on the relevant data user directing the data user to remedy the contravention

• Non-compliance with an enforcement notice commits an offence and carries a penalty of a fine at $50,000 and imprisonment of 2 years

• Same infringement of the second time commits an offence and carries a penalty of a fine at $100,000 and imprisonment of 2 years
Offences (con’t)

• Repeated non-compliance with enforcement notice carries a penalty of a fine at $100,000 and imprisonment of 2 years, in case of a continuing offence, a daily fine of $2,000
• Section 64 provides that “A person commits an offence if the person discloses any personal data of a data subject which was obtained from a data user without the data user’s consent –
  a) With an intent –
    1) to obtain gain in money or other property, whether for the benefit of the person or another person; or
    2) to cause loss in money or other property to the data subject; or
  b) the disclosure causes psychological harm to the data subject.

• Max penalty: a fine of $1,000,000 and 5 years’ imprisonment
Compensation

New section 66B: Privacy Commissioner can grant assistance to data subject in respect of these legal proceedings (effective date 1 April 2013)
Self-training Module on Protection of Personal Data for Medical Practitioners

The Electronic Health Record Sharing System Ordinance (Chapter 625) came into operation on 2 December 2015.

The System launched on 7 March 2016 providing an information infrastructure platform for healthcare providers in both the public and private sectors. With consent of the patient, healthcare providers can have access to and share the patient's health record in the System for healthcare-related purposes.
Electronic Health Record Sharing System

Sharable Data in the System:

The scope of sharable data as of the first quarter of 2016 include the followings:
(a) Personal Identification and Demographic Data (including name, date of birth and identity document number...etc.)
(b) Adverse Reactions and Allergies
(c) Diagnosis, Procedures & Medication
(d) Summary of Episodes and Encounters With Healthcare Providers (i.e. summary of appointments / bookings)
(e) Clinical Note Summary (i.e. Discharge Summary)
(f) Birth and Immunisation Records
(g) Laboratory and Radiology Results
(h) Other Investigation Results
(i) Referral Between Providers
Benefits of the System

• Patient Benefits
  – maintain comprehensive online record for health providers
  – provide timely and accurate information for care
  – reduce duplication of tests and treatment

• Clinician Benefits
  – enable efficient and quality assured clinical practice
  – reduce errors associated with paper records

• Society Benefits
  – improve disease surveillance and monitoring of public health
  – help gather more comprehensive statistics for formulating public health policy
  – bring efficiency gain in total health expenditure
Patients’ health record in the System amounts to personal data, which is protected under the Personal Data (Privacy) Ordinance ("PD(P)O"). Healthcare providers and the Commissioner for Electronic Health Record should act in accordance with the requirements under the PD(P)O (including the Six Data Protection Principles) when handling patients’ health record in the System.

Registered patients can raise a data access request under the PD(P)O to the eHR Registration Office to obtain their health record in the System.
The functions and powers of the Privacy Commissioner for Personal Data, Hong Kong under the PD(P)O in relation to personal data in the System include:

- handling complaints of suspected breaches of the PD(P)O and initiating investigation if necessary
- carrying out an inspection of the System
- providing guidance on personal data privacy in relation to the System to citizens and healthcare providers
- handling any data breach notification in relation to the System

The Relationship between the Personal Data (Privacy) Ordinance and the System
The Electronic Health Record Sharing System Ordinance has introduced offences relating to accessing, damaging or modifying data in the System, for example:

- knowingly obtain unauthorised access to eHR
- knowingly damage eHR
- falsify / conceal eHR to evade DAR / DCR
- use eHR for direct marketing

If the Commissioner for Electronic Health Record receives a case relating to personal data in the System and possible contravention of the PDPO, after obtaining the complainant’s consent, the case will be referred to the PCPD for follow-up.
Three Principles of the System

• Participation of healthcare providers and patients in the System is voluntary, they may withdraw from the System at any time.

• Healthcare providers can only access eHR data of patients under their care with consent.
Three Principles of the System (Con’t)

• Access to eHR on a “need-to-know” principle

• The healthcare provider must take reasonable steps to ensure that—

  (a) access to any health data of the healthcare recipient is restricted to a healthcare professional of the healthcare provider who may perform healthcare for the recipient; and

  (b) the access is restricted to the health data that may be relevant for performing healthcare for the recipient
Privacy and Security Measures

- Role-based Access Control
- Data Validation and Encryption
- Authentication of Patients and Healthcare Providers
- Security Monitoring and Audit
- Code of Practice
- eHR Sharing System Legislation
- Access Notification to Patients
- Restricted Downloading eHR Data
- Safeguard the Patient Rights

Safeguard the Patient Rights

eHR Sharing System

RESTRICTED DOWNLOADING eHR DATA

ACCESS NOTIFICATION TO PATIENTS

EHR SHARING SYSTEM LEGISLATION

DATA VALIDATION AND ENCRYPTION

SECURITY MONITORING AND AUDIT

AUTHENTICATION OF PATIENTS AND HEALTHCARE PROVIDERS

CODE OF PRACTICE
Information Leaflet for the Public

Electronic Health Record Sharing System and Your Personal Data Privacy

[10 Privacy Protection Tips]

Information Leaflet for the Public

• Ten Privacy Protection Tips

1. Limited scope of sharable data

➢ healthcare providers can only access to the data within the pre-defined scope of eHR sharable data (not all the personal data provided during treatment). Hence, before joining the System, participant should ascertain the scope of sharable data from healthcare providers.
Information Leaflet for the Public

• Ten Privacy Protection Tips

2. Clear understanding before joining

➢ read the Personal Information Collection Statement, Privacy Policy Statement and Participant Information Notice carefully provided by the Commissioner for the Electronic Health Record

➢ read the privacy policy of a healthcare provider carefully to understand how the personal data will be processed in the System, as the privacy policies vary between healthcare providers
Information Leaflet for the Public

• Ten Privacy Protection Tips

3. Cautious consideration before giving consent

➢ if there are any questions about the collection, processing and protection of personal data in the System, participant should clarify them with eHR Registration Centres or healthcare providers

➢ healthcare providers may access patients’ eHR on the “need-to-know” principle. Hence, participant must cautiously consider and decide
Information Leaflet for the Public

• Ten Privacy Protection Tips

4. Right to revoke consent at any time

 participant may withdraw from the System and revoke his sharing consent given to any healthcare providers by making an application to the Commissioner for the Electronic Health Record at any time

 as it takes time to process revocation or withdrawal request, if participant need to receive treatment during this processing period, he should inform the healthcare provider of his applications for revocation or withdrawal. The healthcare provider should respect his decision
Information Leaflet for the Public

• Ten Privacy Protection Tips

5. Maintaining consent record

➢ after consent has been given, the System will send the participant a notification by a means chosen by the participant (e.g. SMS). Participant may record the details of the sharing consent given to healthcare providers for future reference

6. Right to access data

➢ participant can make a data access request ("DAR") to the Commissioner for the Electronic Health Record to obtain his personal data in the System
Information Leaflet for the Public

• Ten Privacy Protection Tips

6. Right to access data (con’t)
   ▶ participant can make a DAR to an individual healthcare provider for accessing his personal data in its local system

7. Safekeeping of data
   ▶ participant must safeguard the copies of eHR (in paper form or otherwise) obtained in a data access request to avoid leakage of personal data
8. Right to correct data

- if participant find his personal data accessed via the above channel to be inaccurate, he may request for data correction by writing to the Commissioner for the Electronic Health Record
- however, as the eHR in the System is provided and uploaded by healthcare providers, participant may make enquiries with the healthcare provider concerned first
9. Paying attention to access notification

- All access activities will be logged in the System. The System sends notification by a means chosen by participant whenever their eHR is accessed.
- Notify the Commissioner for the Electronic Health Record immediately, or make enquiries with the healthcare provider concerned if participant suspect their eHR is accessed by an unauthorised party.
10. Giving consent on behalf of minors or persons incapable of managing their own affairs

- consent must be given by the participant himself, unless the participant is a minor (aged below 16) or a person incapable of managing his own affairs

- for the above person, his parents, guardians, person appointed by court, his family member or a person residing with them, or a prescribed healthcare provider will act as a substitute decision maker, who should make decisions in the best interest of the above person
Information Leaflet for Healthcare Providers and Healthcare Professionals

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' 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, 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.che-health.gov.hk) for more details.

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

Patients' health records in the System are so sensitive that the Personal Data (Privacy) Ordinance protects them. Healthcare providers and the Commissioner for the Electronic Health Record, as 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 Data Protection Principle) 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 and initiating investigation if necessary;
- Chapter 4 of the Law of Hong Kong
  Chapter 4 of the Law of Hong Kong
  Chapter 4 of the Law of Hong Kong

Information Leaflet for Healthcare Providers and Healthcare Professionals

• Points to Note for Healthcare Providers and Healthcare Professionals

1. Patients’ participation and giving of sharing consent

➢ health records are sensitive personal data. Healthcare providers should patiently explain the operation of the System to patients in detail

➢ remind patients to read carefully the “Participant Information Notice” issued by the Commissioner for the Electronic Health Record about the details of the System
Information Leaflet for Healthcare Providers and Healthcare Professionals

• Points to Note for Healthcare Providers and Healthcare Professionals

2. Access to eHR on a “need-to-know” principle
   - set adequate but not excessive access right to the data in the System
   - incorporate the requirement of keeping patient’s information confidential in staff manual or code of practice
   - exercise professional judgment to determine what exact data is necessary to be accessed
Information Leaflet for Healthcare Providers and Healthcare Professionals

• Points to Note for Healthcare Providers and Healthcare Professionals

3. Data accuracy

➢ should ensure that the eHR provided to the System by them are accurate and comply with the sharing requirements
4. Data security

- shall adopt all reasonably practicable steps to protect the personal data in the System. For example
  - eHR shown on the computer screen will not be seen by unrelated third parties
  - adopt appropriate measures to ensure that healthcare providers’ data systems are adequately safeguard
- notify the Commissioner for the Electronic Health Record and the Privacy Commissioner for Personal Data as soon as possible if there is data breach of the System/PCPD (though not mandatory)
Information Leaflet for Healthcare Providers and Healthcare Professionals

• Points to Note for Healthcare Providers and Healthcare Professionals

5. Direct Marketing

➢ using eHR in the System in direct marketing is a criminal offence under the Electronic Health Record Sharing System Ordinance

➢ 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
Information Leaflet for Healthcare Providers and Healthcare Professionals

• Points to Note for Healthcare Providers and Healthcare Professionals

6. Personal data privacy policy
   ➢ should review their existing personal data privacy policies and make amendments accordingly

7. Data access requests/data correction requests
   ➢ 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 PD(P)O
Information Leaflet for Healthcare Providers and Healthcare Professionals

• Points to Note for Healthcare Providers and Healthcare Professionals

7. Data access requests/data correction requests (con’t)

➢ 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 PD(P)O

➢ 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 PD(P)O
Information Leaflet for Healthcare Providers and Healthcare Professionals

• Points to Note for Healthcare Providers and Healthcare Professionals

8. Complaint handling

- it is within the jurisdiction of the PCPD to handle complaints relating to personal data in the System (irrespective of whether it is lodged with the PCPD directly or referred to by the Commissioner for the Electronic Health Record), the PCPD will follow them up according to its Complaint Handling Policy
Information Leaflet for Healthcare Providers and Healthcare Professionals

- Action List for Healthcare Providers before joining the System for Protection of Personal Data Privacy
  - 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
Personal Information Collection Statement (PICS)

Example:
• “When you visit this website, we may use cookie files to store and track information about your (details to be specified by the data user) or your actions for the purposes of providing our services to you on/for (details to be specified by the data user).”

Examples:
• “The information collected from you will be used for the purpose of processing your purchase orders and managing your account with us.”

• “The information collected by means of cookies on this website about you will be used only for compiling aggregate statistics on how visitors browse the website. Such statistics are collected for the purpose of managing and improving the design of the website.”

• “Your name and address will be used by our leisure club for sending you newsletters and printed material about our recreational events for promoting healthy lifestyle.”

Example:
• “Please note that it is mandatory for you to provide personal data marked with asterisks. In the event that you do not provide such personal data, we may not be able to provide you with our products or services.”

• “Please provide your telephone number in case we need to contact you about your comments on our services. You do not have to tell us your phone number but it will help us to contact you quickly if we have a question about your comments.”

• “Where cookies are used on websites to collect information about visitors: “Most web browsers are initially set up to accept cookies. You can choose to ‘not accept’ cookies by changing the settings but if you do so you may find that certain features on the website, including online banking, do not work properly.”

Example:
• “For the purposes of providing membership services to you, the information that we collect about you will be published through our website or made available for public access through our registration office.”
Personal Information Collection Statement (PICS)

Example of a PICS given by a society or an association which offers special discounts on goods and services (e.g. recreational activities) to individuals who are interested to subscribe or participate:

- "Your name, mobile phone number and home address collected by us will be used for providing you with information about recreational activities and special offers on household goods, food and entertainment to be provided or sponsored by us.

We cannot use your personal data unless we have received your consent or indication of no objection."

Please indicate your consent to receiving information relating to the above by signing and returning to us this Form by Fax # 1234 5678 or by sending it to any of our liaison offices.

________________________
Name and signature
(dd/mm/yyyy)

or

If you do not wish to receive information on the above, please tick the box below:

☐ I object to the proposed use of my personal data as stated above.

________________________
Name and signature
(dd/mm/yyyy)

(In both cases the data user may not use the personal data for direct marketing purpose unless a signed form is returned. In the latter case, if the form is returned with a signature but without a tick, it may be considered as an “indication of no objection”.)

Example:

- "You have the right to request access to and correction of information held by us about you. If you wish to access or correct your personal data, please contact our data protection officer at ‘1/F, No.1 Main Road, Hong Kong’ or dpo@company.com.”
Privacy Policy Statement (PPS)

Examples:

- “We are committed to protecting the privacy, confidentiality and security of the personal information we hold by complying with the requirements of Personal Data (Privacy) Ordinance with respect to the management of personal information. We are equally committed to ensuring that all our employees and agents uphold these obligations.”

- “We pledge to comply with the requirements of the Personal Data (Privacy) Ordinance. In doing so, we will ensure compliance by our staff with the strictest standards of security and confidentiality.”

Examples:

- “Your personal details, job particulars, salary and benefits, appraisal and disciplinary records collected and held by us will be used for the purpose of human resource management.”

- “We will not provide your personal data to third parties for direct marketing or other unrelated purposes without your consent.”
Privacy Management Programme

- Paradigm shift from compliance to accountability
- Embrace personal data protection as an integral part of corporate governance
- Implement it throughout their organisations
Privacy Management Programme Pledging Organisations

Media Statements
Date: 18 February 2014

Major Organisations Pledge to Implement Privacy Management Programme to Protect Personal Data Privacy

(18 February 2014)

At a ceremony held today by the PCPD, the Hong Kong Special Administrative Region Government, together with twenty five companies from the insurance sector, nine companies from the telecommunications sector and five organisations from other sectors, all pledged to implement PMP.
Media Statements
Date: 18 February 2014

Major Organisations Pledge to Implement Privacy Management Programme to Protect Personal Data Privacy

PMP Best Practice Guide Framework

• Three top-down management commitments

➢ top management buy-in of the PMP

➢ appointment of a Data Protection Officer or Office

➢ internal reporting mechanism
PMP Best Practice Guide Framework

• Seven bottom-up programme controls
  - a personal data inventory
  - internal policies (DPPs)
  - risk assessment
  - up-to-date training and education
  - procedure of notification (data breach)
  - obligations for data processor
  - communication with employees and customers

• Two on-going monitoring processes
  - local
  - overseas
thank you