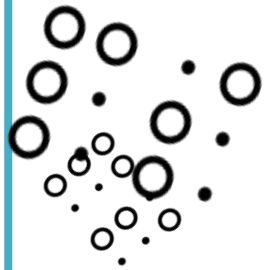
Seminar on Cyber Security and Personal Data Privacy Protection in eHealth

Privacy Protection & Data Security in Digital Healthcare Environment
數碼醫療環境的私隱保障與數據安全

24 October 2025

The values of personal data

- Personal data holds significant economic and social value as a key resource in the digital economy, powering personalized services, innovation, and research.
- Businesses use it to understand consumers, tailor ads, develop products, and train AI, while it also improves public services.



2025 Policy Address: *"AI is the key driving force of a new round of scientific and technological revolution, as well as industrial transformation. …. We will promote the development of AI+ and facilitate an extensive and deep integration of AI across sectors, with a view to achieving "**industries for AI**" and "**AI for industries**", while placing strong emphasis on safety risk prevention."*

Data sharing that benefits the society

- **2024 Policy Address**: Setting up an inter-disciplinary and interorganisation database on carers of elderly persons and carers of persons with disabilities, with a view to identifying high-risk cases for early intervention and support.
- A database on carers was rolled out in July 2025, allowing the Government to use data to identify families at risk at an earlier stage.

Hong Kong to launch pilot project to identify at-risk carers in coming weeks

Welfare minister says scheme to be launched in two phases, with first stage using Hospital Authority data to flag if carers have been hospitalised

Source: SCMP, 5-7-2025

General Requirements of Personal Data Protection

6 Data Protection Principles (DPPs)

- Represent the core requirements of the Personal Data (Privacy) Ordinance, Chapter 486 of the Laws of Hong Kong (PDPO)
- Cover the entire lifecycle of personal data from collection, holding, processing, use to deletion
- Data users have to comply with the DPPs

6 DPPs
DPP1 Purpose and Manner of Collection of Personal Data

- Must be collected for a lawful purpose directly related to a function or activity of the data user
- The means of collection must be lawful and fair
- The data is adequate but not excessive in relation to the purpose of collection
- All practical steps shall be taken to notify the data subjects whether it is obligatory to supply the personal data , the purpose of data collection, and the classes of persons to whom the data may be transferred, etc.

6 DPPs
DPP2 Accuracy and Duration of Retention of Personal Data

- Data users should take all practicable steps to ensure:
  - the accuracy of the personal data
  - the personal data is not kept longer than is necessary for the fulfilment of the purpose for which the data is used
- If a data processor is engaged to process personal data, the data user must adopt contractual or other means to prevent the personal data from being kept longer than is necessary

6 DPPs
DPP3 Use of Personal Data

- **Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose**

  "*New purpose*" means any purpose which is *unrelated to the original purpose or its directly related purpose* when the data is collected

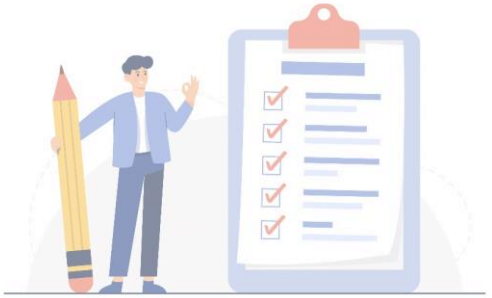
- **Under certain circumstances, a relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using the data subject's personal data for a new purpose**

6 DPPs
DPP4 Security of Personal Data

- Data users should take all practicable steps to ensure the personal data they hold is protected against unauthorized or accidental access, processing, erasure, loss or use
- Adequate protection must be given to the storage, processing and transfer of personal data
- If a data processor is engaged, the data user must adopt contractual or other means to prevent unauthorized accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing

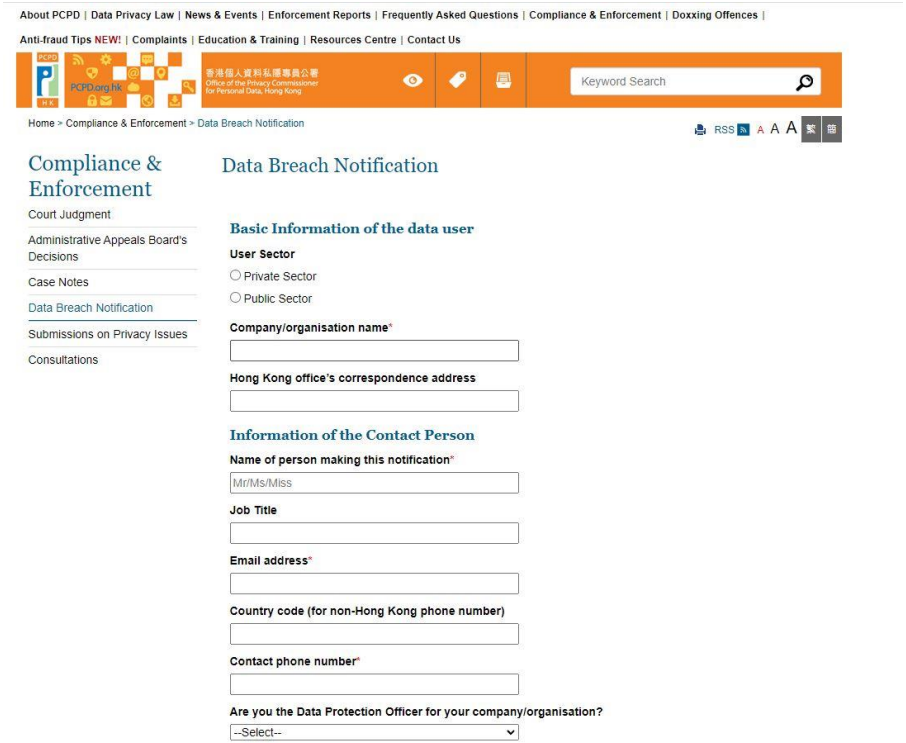
6 DPPs
DPP4 Security of Personal Data (cont'd)

Practicable Steps



Data users should consider: -

1) the kind of data and the harm that could result;
2) physical location where the data is stored;
3) any security measures incorporated into any equipment in which the data is stored;
4) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
5) any measures taken for ensuring secure transmission of the data.



e-Data Breach Notification Form

since June 2023

www.pcpd.org.hk

Home > Compliance and Enforcement > Data Breach Notification

Guidance on Data Breach Handling and Data Breach Notifications

INTRODUCTION

Good data breach handling makes good business sense

A good data breach handling policy and practice is not only useful for containing the damage caused by a breach, but also demonstrate the data user's responsibility and accountability when tackling the problem, by formulating a clear action plan that can be followed in the event of a data breach. In addition to enabling the data subjects affected by the breach to take appropriate protective measures, data breach notifications can help reduce the risk of litigation and maintain the data user's goodwill and business relationships, and in some cases the public's confidence in the organisation.

This guidance is aimed at assisting data users to prepare for and handle data breaches, to prevent recurrence and to mitigate the loss and damage caused to the data subjects involved, particularly

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable.

What is a data breach?

A data breach is generally regarded as a suspected or actual breach of the security of personal data held by a data user[2], which exposes the personal data of data subject(s) to the risk of unauthorised or accidental access, processing, erasure, loss or use.

The following are some examples of data breaches:

- The loss of personal data stored on devices such as laptop computers, USB flash drives, portable hard disks or backup tapes

Revised in June 2023

6 DPPs
DPP5 Information to be Generally Available

Transparency

Data users must provide information on: -

1) the policies and practices in relation to personal data;
2) the kind of personal data held; and
3) the main purposes for which personal data is used.

6 DPPs
DPP6 Access to Personal Data

Data subject's rights

A data subject must be given access to his personal data and to request corrections where the data is inaccurate

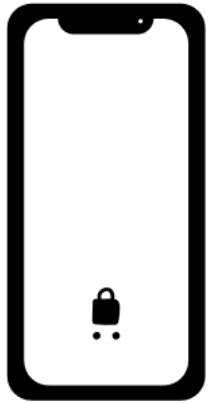
A data user must comply with a data access/correction request within 40 days after receipt of the request

(Sections 19 and 23 of the PDPO)

Case Sharing (1)
Data collection – Requesting information for handling telephone enquiry

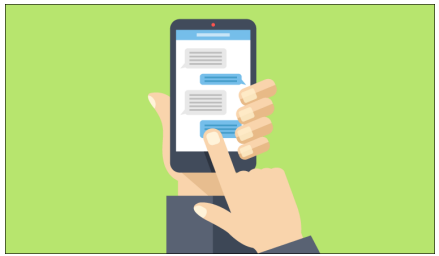
- The complainant called the hotline of a hospital for enquiry.

- The complainant was dissatisfied that the hotline staff asked for his HKID number and name whilst his enquiry was general in nature.



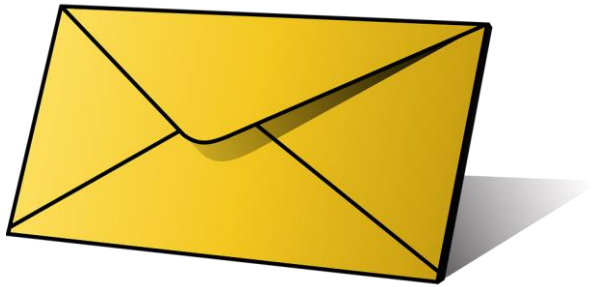
Case Sharing (2)
Use of personal data - Accessing patient's electronic health record for non-medical purposes

- The complainant gave consent to a hospital to upload and access his health record via the eHRSS.
- After a visit, the complainant made a complaint against the attending doctor to a regulatory body.
- While the complainant's case was being handled, the Complainant received a text message from the eHR Office, informing him that the doctor had accessed his electronic health record.



Case Sharing (3)
Data security – Too much information on envelop

- A clinic sent a letter to the complainant's home address by post.
- The logo and chop on the envelop are indicative of the identity of the sender.
- The complainant was dissatisfied that there was too much information on the envelop, such that his family members were aware that he was receiving medical treatment.



Case Sharing (4)

Data security – Failing to log out before leaving

- After performing an ultrasound scan on the complainant, the doctor of a medical diagnostic centre did not log out of the system before leaving the examination room.
- As a result, the complainant who remained in the examination room was able to read the information of other patients displayed on the screen of the examination equipment, including the English names, the full HKID numbers and brief medical histories of the patients concerned.

Beware….

Trending in China *People & Culture / Trending in China*

Chinese man's affair exposed after birth control pills e-payment fails; pharmacy notifies wife

Man claims incident resulted in collapse of two families, demanding accountability from pharmacy

Source: SCMP, 22-8-2025

Thank you!

Telephone： 2827 2827

Website： www.pcpd.org.hk

Email： communications@pcpd.org.hk