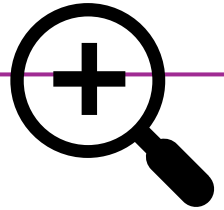
Privacy Protection & Data Security in Digital Healthcare Environment

數碼醫療環境的私隱保障與數據安全

Webinar on Cyber Security and Personal Data Privacy Protection in eHRSS

21 October 2024

New Developments



eHealth

- ✓ As of the end of May 2024, there are approximately six million registered individual users on eHealth, covering nearly 80 per cent of the total population in Hong Kong.
- ✓ Over 4.02 billion sharable eHRs on eHealth
- ✓ eHealth+: One Health Record, One Care Journey, One Digital Front Door to Empowering Tool and One Health Data Repository.
- ✓ New functions on eHealth App: "Cross-boundary Health Record" and "Personal Folder"

Source: HKSAR Government Press Release, 20-6-2024, 26-6-2024

General Requirements of Personal Data Protection

6 Data Protection Principles (DPPs)

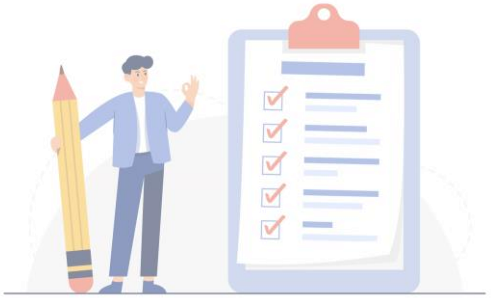
- Represent the core requirements of the Personal Data (Privacy) Ordinance, Chapter 486 of the Laws of Hong Kong (PDPO)
- Cover the entire lifecycle of personal data from collection, holding, processing, use to deletion
- Data users have to comply with the DPPs

6 DPPs
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



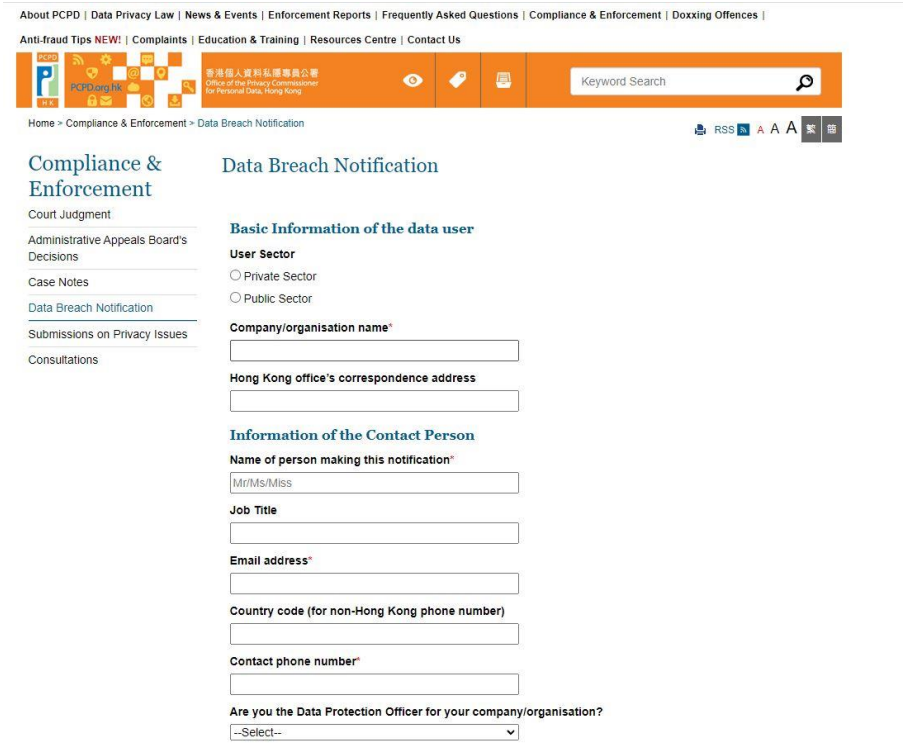
Data users should consider: -

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.

Recommended Practice for Handling Data Breach

- Step 1: Immediate gathering of essential information
- Step 2: Containing the data breach
- Step 3: Assessing the risk of harm
- Step 4: Considering giving data breach notifications
- Step 5: Documenting the breach

Organisations should notify the PCPD and the affected data subjects as soon as practicable after becoming aware of the data breach, particularly if the data breach is likely to result in a real risk of harm to those affected data subjects.



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

Case Sharing (1)
Data security – Handling of patients' wrist bands

- While the complainant was hospitalized, he made a brief return to home. His wrist band was removed before leaving.
- When the complainant came back to the hospital, he found that his wrist band was placed on the bedside cabinet.
- The complainant was dissatisfied that his personal data printed on the wrist band was exposed to other patients.

Case Sharing (2)
Data security – Handling of letters to patients

- A clinic sent a letter to the complainant's home address informing him of the consultation arrangement.
- The letter was found not sealed. It was also not enveloped.
- The complainant was dissatisfied that his personal data printed on the letter could be checked by his family members who passed him the letter.

Data security

- Data Protection Principle 4 provides that all practicable steps shall be taken by a data user to ensure that any personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use.

- Generally speaking, measures shall be taken to enhance the security of personal data, in particular for sensitive personal data e.g. medical data, HKID number.

Thank you!

Telephone： 2827 2827

Website： www.pcpd.org.hk

Email： communications@pcpd.org.hk