Webinar on Cyber Security and Personal Data Privacy Protection in eHRSS

14 October 2022

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

PCPD HK

PCPD.org.hk

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

Outline

01 **DIGITAL HEALTHCARE TRENDS**

- AI, Telemedicine & Cloud Computing

02 **PRIVACY AND ETHICAL RISKS**

- Collection of Data, Biased AI, Data Security, etc.

03 **DATA PROTECTION REQUIREMENTS IN HK**

- Key Definitions, 6 Data Protection Principles (DPPs) & Case Sharing

04 **GUIDANCE MATERIALS**

- Ethical AI & Data Protection by Design

01 DIGITAL HEALTHCARE TRENDS

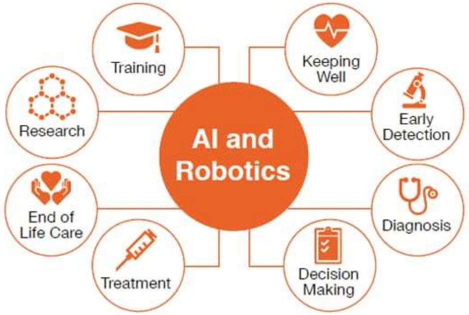
Healthcare and AI

Artificial Intelligence

- Artificial Intelligence (AI) is getting sophisticated at mimicking human's capability

✓ **Machine learning**:
AI is capable of digesting a vast amount of data, enabling accurate and early diagnosis

✓ **Automated Robots**:
AI handles repetitive tasks accurately and tirelessly



AI and Robotics

Training

Keeping Well

Early Detection

Diagnosis

Decision Making

Treatment

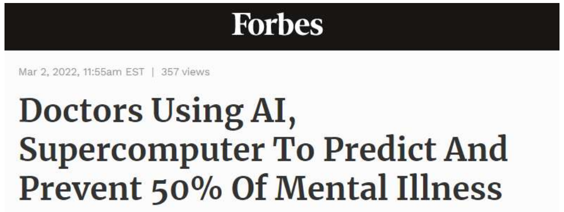
End of Life Care

Research

Source: PwC, 2017

Studies prove that AI is on a par with healthcare professionals when diagnosing illnesses

AI is beneficial to the whole healthcare eco-system



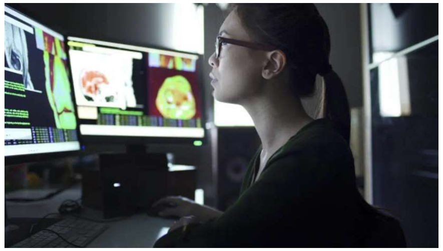
Forbes

Mar 2, 2022, 11:55am EST | 357 views

Doctors Using AI, Supercomputer To Predict And Prevent 50% Of Mental Illness

Source: Forbes, 2022

AI just as good at diagnosing illness as humans



Source: Medical News Today, 2019

Telemedicine

Telemedicine

- Telemedicine has gained popularity worldwide as a result of the COVID-19 pandemic

✓ **Easy-accessible** and **cost effective** medical consultations

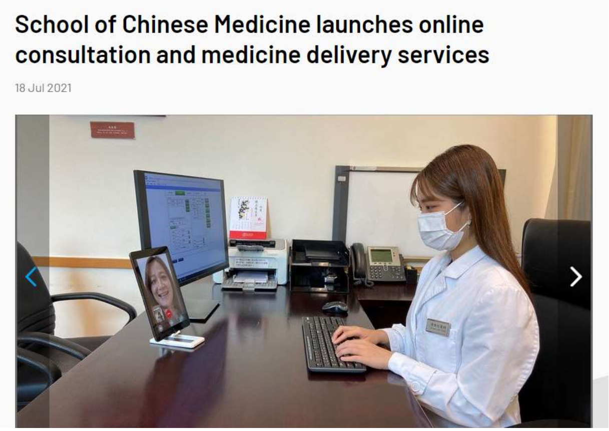
What is TeleHealth via HA Go?

With HA Go, patients can attend a clinic appointment at home remotely #

#Available at designated clinics only

In Hong Kong, Hospital Authority (HA) launched TeleHealth pilot programme

HKBU's Chinese medicine clinic is also working on online consultation



School of Chinese Medicine launches online consultation and medicine delivery services

18 Jul 2021

Source: BU News, 2021

Cloud Computing

Cloud Computing

- Cloud computing offers a centralised and offsite storage system

✓ **Cost-efficiency**: data storage cost would be lowered

✓ **Flexible subscription**: unlike physical machines, a cloud storage system can scale up and down

✓ **Big data analytics**: large sets of data enable and facilitate data analytics

Cloud computing in healthcare is growing fast in APAC – here's why

Source: Techwire Asia, 2021

The Asia Pacific region is anticipated to be the fastest-growing regional market of healthcare digitalisation

For example, the Singapore government launched "Healthcare-Cloud" to support 9 public hospitals, which helps to reduce 55% operational costs by 2025

H-Cloud Data Centres: Supporting Healthcare Operations in Singapore

5,000 servers
1 Petabyte storage
Over 350 network, security & network equipment

Source: IHiS

02 PRIVACY AND ETHICAL RISKS

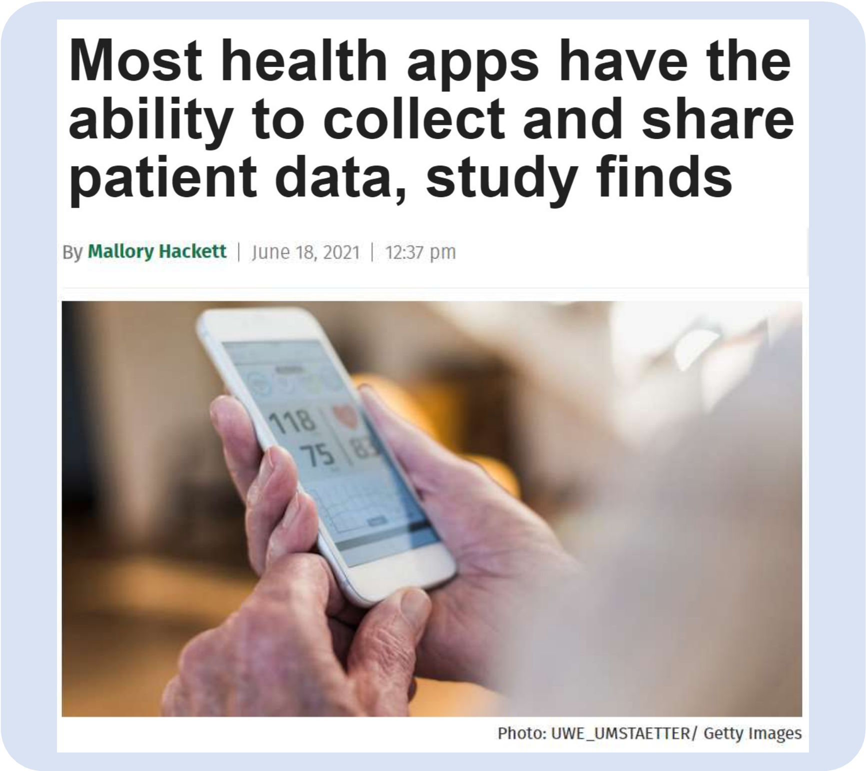
Privacy and Ethical Risks

1) Collection & Use of Data

- Personal data, including health data, is more valuable than ever
- Health data may be processed, transferred or even used for a new purpose

➢ A study finds that 88% of health apps can collect and potentially share user data

➢ 56% of data transmissions go to 3rd parties which include adverts, analytics and other services



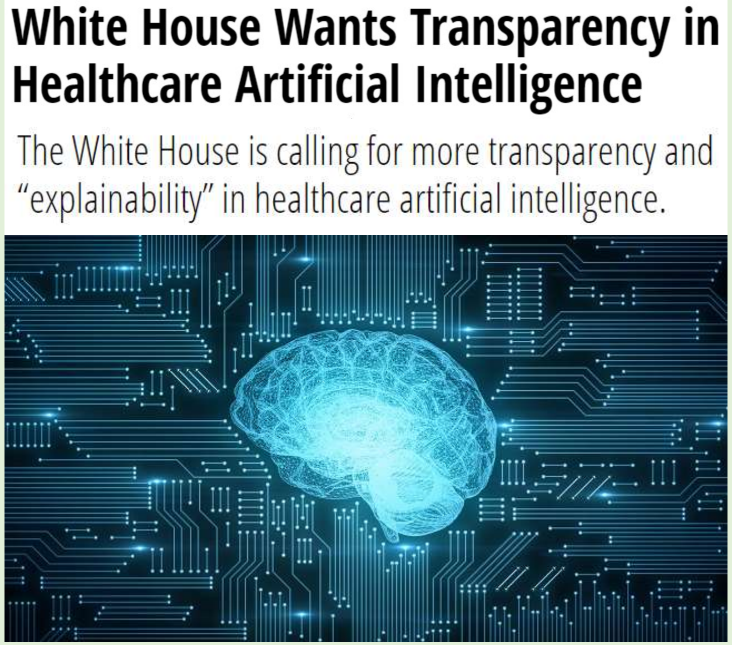
Most health apps have the ability to collect and share patient data, study finds

By Mallory Hackett | June 18, 2021 | 12:37 pm

Photo: UWE_UMSTAETTER/ Getty Images

Source: mobihealthnews, 2021

Privacy and Ethical Risks



White House Wants Transparency in Healthcare Artificial Intelligence

The White House is calling for more transparency and "explainability" in healthcare artificial intelligence.

Source: HITInfrastructure, 2019

2) Lack of Transparency

- AI algorithms sometimes evolve beyond our comprehension

- Processing of data and decision-making process may take place in a "**black-box**"

➢ In 2019, the U.S. National Science and Technology Council released a strategic plan urging researchers to develop systems that are **transparent** and **intrinsically capable of explaining** their results, **particularly in healthcare**

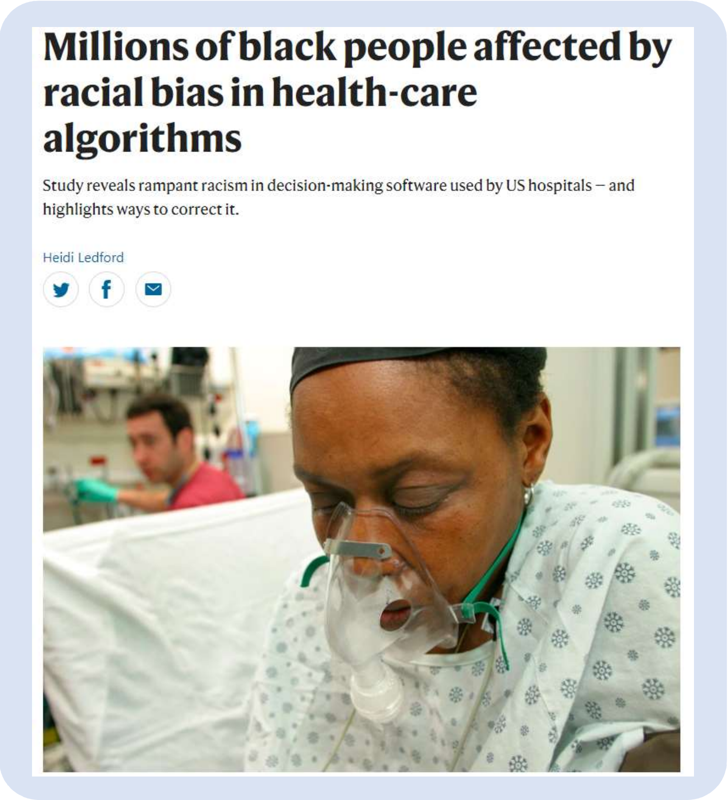
Privacy and Ethical Risks

3a) Bias and Discrimination – Biased Inputs

- Unexpected discrimination may occur if the inputs in the first place are unintentionally biased

➢ A study on algorithms finds that dark-skinned people were **less likely** to be referred to the personalised care programme

➢ One of the inputs is “**medical expense**”, where poorer dark-skinned people were **wrongly classified** as “less in need” for care just because they spent less **in the past**



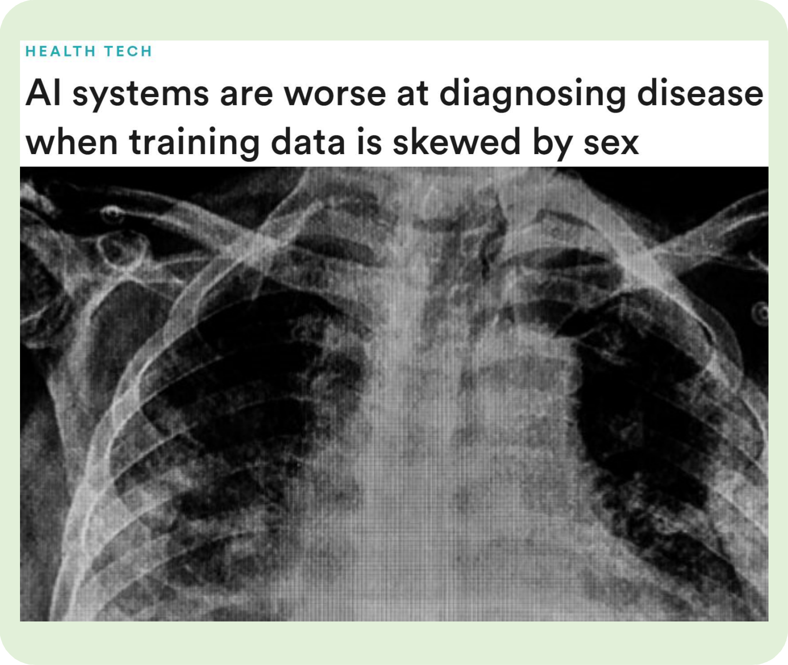
Millions of black people affected by racial bias in health-care algorithms

Study reveals rampant racism in decision-making software used by US hospitals – and highlights ways to correct it.

Heidi Ledford

Source: Nature, 2019

Privacy and Ethical Risks



HEALTH TECH

AI systems are worse at diagnosing disease when training data is skewed by sex

Source: STAT, 2020

3b) Bias and Discrimination – Skewed Data

- AI systems also rely on **training data** to acquire their “intelligence”
- If training datasets are **skewed** and **dominated** by a particular group, AI systems may be **unreliable**, especially when applying to **minorities**

➢ An AI model was designed for predicting patients’ acute loss of kidney function while only about **6%** of training data were from women patients

➢ The model was found to perform worse when applied to the **underrepresented**

Privacy and Ethical Risks

4) Security of Health Data

- Health data is "going online", especially when telemedicine technology and cloud computing were widely adopted

- Health data stored online may fall prey to hackers

➢ Healthcare has been the **most affected sector** of personal data breaches

➢ In the UK, the healthcare sector reported the highest number (**435** or **18%)** of data breaches among all industries
[Source: UK Information Commissioner's Office, Data Security Incident Trends for Q2 2021/22]

The biggest healthcare data breaches of 2021

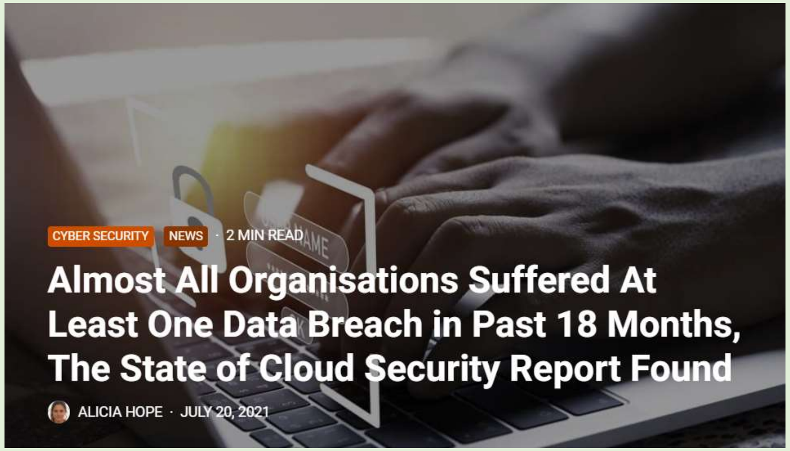
More than 40 million patient records have been compromised this past year by incidents reported to the federal government in 2021.

By Kat Jercich | November 16, 2021 | 09:54 AM

Photo: cottonbro/Pexels

Source: Healthcare IT News, 2021

Privacy and Ethical Risks



CYBER SECURITY NEWS · 2 MIN READ

Almost All Organisations Suffered At Least One Data Breach in Past 18 Months, The State of Cloud Security Report Found

ALICIA HOPE · JULY 20, 2021

Source: CPO Magazine, 2021

5) Loss of Control due to Outsourcing

- Technical support services are often **outsourced** in order to boost efficiency e.g.:
  a) Saving patients' health data to **cloud storage**
  b) Providing telemedicine consultations by using **videoconferencing apps**

➢ A report shows that almost **all** companies experienced a cloud data breach

03 DATA PROTECTION REQUIREMENTS IN HONG KONG

What is Personal Data?

Section 2(1) of Personal Data (Privacy) Ordinance

Personal Data means any data -

a)Relating directly or indirectly to a living individual;

a)Practicable for the identity of the individual to be directly or indirectly ascertained; and

a)In a form in which access to or processing of the data is practicable

Who are involved?

Personal Data (Privacy) Ordinance:

- The individual who is the subject of the data

Data Subject

- A person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data;

Data User

A person who –

a) Processes personal data on behalf of another person; and

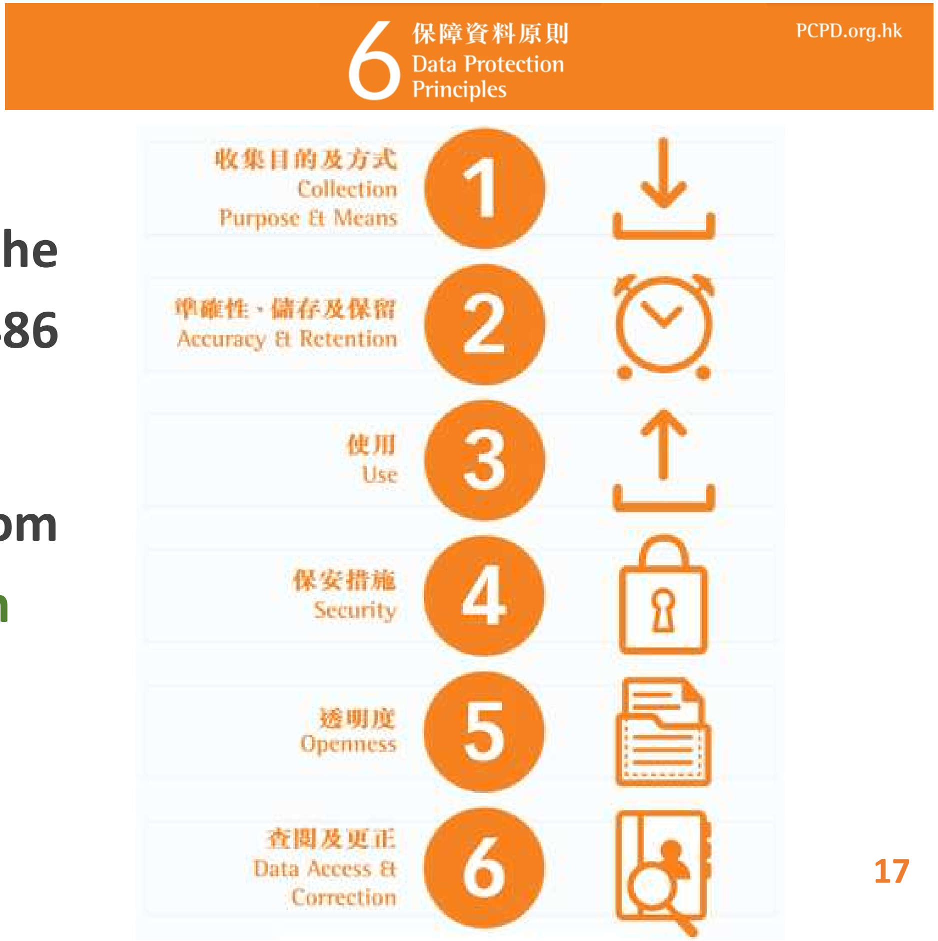
b) Does not process the data for any of the person's own purposes

Data Processor

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**

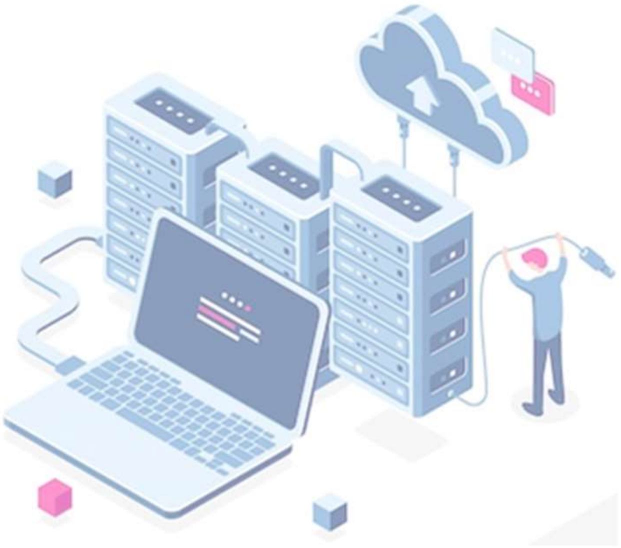
“*New purpose* ” means any purpose which is *unrelated to the original purpose or its directly related purpose* when the data is collected

- **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

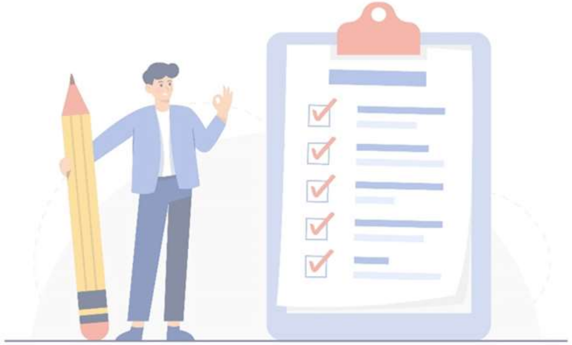
- Data users should take **all practicable steps** to ensure the personal data they hold is protected against **unauthorized or accidental access, processing, erasure, loss or use**
- **Adequate protection** must be given to the storage, processing and transfer of personal data
- If a **data processor** 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: -

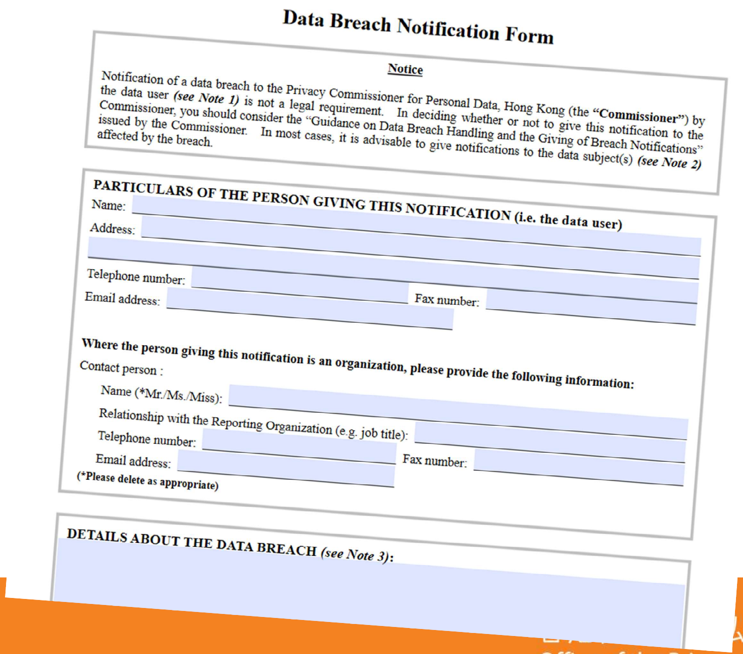


1) the kind of data and the harm that could result;
2) physical location where the data is stored;
3) any security measures incorporated into any equipment in which the data is stored;
4) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and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

Recommended Practice for Handling Data Breach

- Collect essential information immediately
- Assess the impact on data subjects
- Adopt containment measures
- Contact stakeholders (e.g. services provider, management and affected data subjects)
- Give data breach notification to PCPD

To: Privacy Commissioner for Personal Data, Hong Kong



Data Breach Notification Form

Notice

Notification of a data breach to the Privacy Commissioner for Personal Data, Hong Kong (the "**Commissioner**") by the data user ***(see Note 1)*** is not a legal requirement. In deciding whether or not to give this notification to the Commissioner, you should consider the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the Commissioner. In most cases, it is advisable to give notifications to the data subject(s) ***(see Note 2)*** affected by the breach.

PARTICULARS OF THE PERSON GIVING THIS NOTIFICATION (i.e. the data user)

Name:

Address:

Telephone number:

Email address: Fax number:

Where the person giving this notification is an organization, please provide the following information:

Contact person :

Name (*Mr./Ms./Miss):

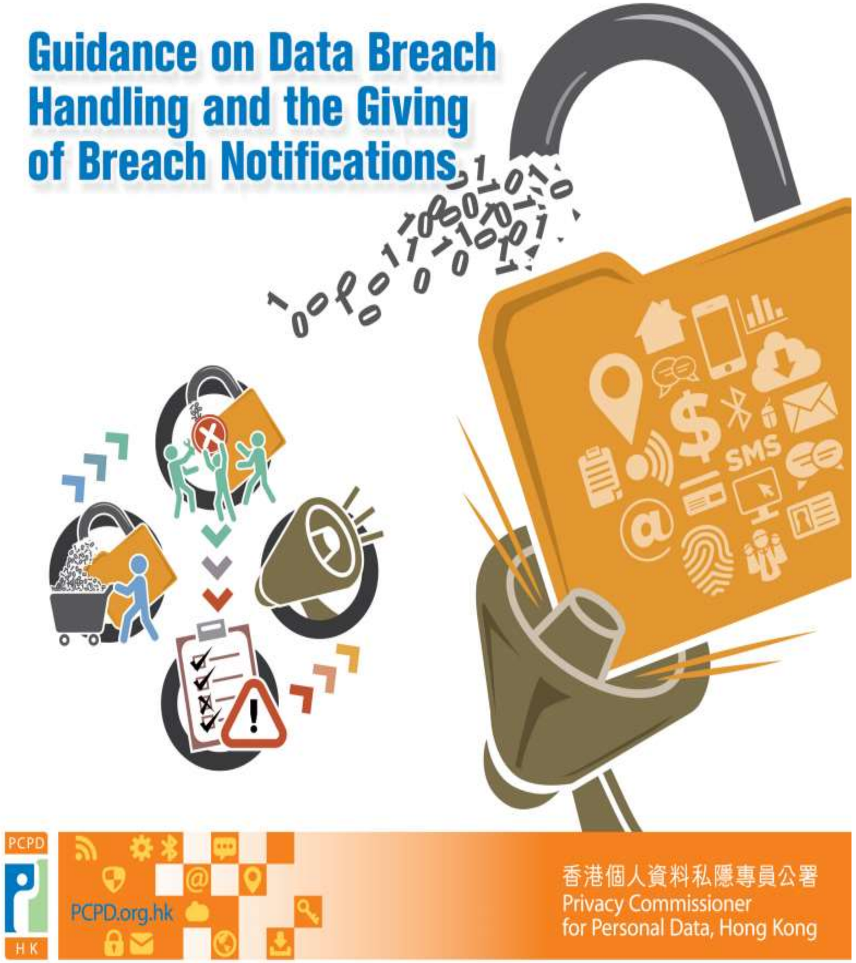
Relationship with the Reporting Organization (e.g. job title):

Telephone number:

Email address: Fax number:

(*Please delete as appropriate)

DETAILS ABOUT THE DATA BREACH *(see Note 3)*:



Guidance on Data Breach Handling and the Giving of Breach Notifications

PCPD
HK

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

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

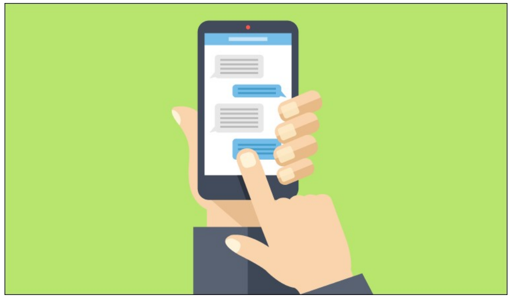
A data subject must be given access to his personal data and to request corrections where the data is inaccurate

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)
Accessing patient's electronic health record for non-medical purposes

- The Complainant gave consent to a Doctor to upload and access his health record via the eHRSS.
- After a visit, the Complainant made a complaint against the Doctor to the Medical Council of Hong Kong.
- While the Medical Council was handling the Complainant's case, the Complainant received a text message from the eHR Office, informing him that the Doctor had accessed his electronic health record.



Case Sharing (1)
Accessing patient's electronic health record for non-medical purposes

- Accessing the Complainant’s electronic health record in the eHRSS for a purpose other than providing treatment to the Complainant and without obtaining separate consent from the Complainant → Contravention of DPP3
- Remedial action taken by the Doctor
  - ✓ undertook to access eHRSS only for the purpose of providing treatment to patients and on a "need-to-know" basis
- A warning was issued to the Doctor
- Also referred the case to the eHR Office

Case Sharing (2)
Being registered eHRSS without consent

- The Complainant booked the COVID-19 Vaccination via the online booking system. He did not indicate his wish to register eHRSS during the booking.
- On the day of vaccination, the Complainant did not indicate his wish to register eHRSS on the information leaflet as well.
- After vaccination, the Complainant received a SMS stating that he had registered eHRSS.

Case Sharing (2)
Being registered eHRSS without consent

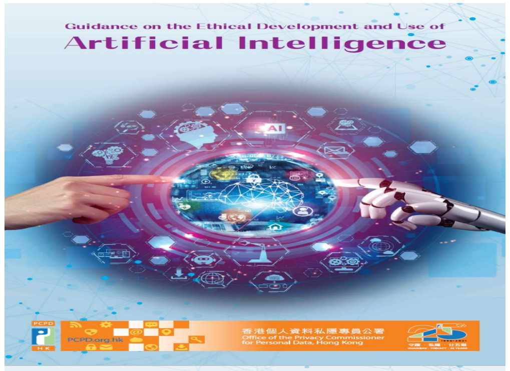
- Investigation revealed that when processing the vaccination registration for the Complainant in the vaccination system, a staff member of the services provider had ticked the checkbox of registering eHRSS for the Complainant by mistake.
- Using the Complainant's personal data to register eHRSS → a purpose other than processing vaccination registration for the Complainant and without obtaining the Complainant's consent → Contravention of DPP3
- Remedial actions:
  - ✓ Formulate guideline
  - ✓ Reminder to all staff
  - ✓ Arrange senior staff for random check
- A warning was issued to the service provider
- Contact eHR office to relay the Complainant's request for deleting his eHRSS account

04 GUIDANCE MATERIALS

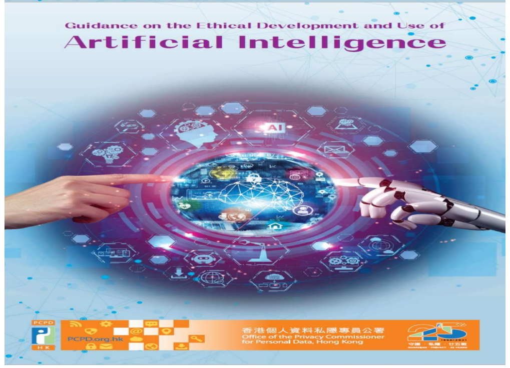
PCPD’s Guidance on the Ethical Development and Use of Artificial Intelligence

Objectives

- To provide guidance to enable organisations to develop and use AI in compliance with the requirements under the PDPO and in an ethical manner
- To facilitate healthy development and use of AI in Hong Kong
- To facilitate Hong Kong to become an innovation and technology hub and world-class smart city



Guidance on the Ethical Development and Use of
Artificial Intelligence



Guidance on the Ethical Development and Use of
Artificial Intelligence

Guide to Data Protection by Design for ICT Systems

Overview

- **Data Protection by Design (DPbD)**: To consider and build data protection measures into ICT systems that process personal data in the development stage

Objectives

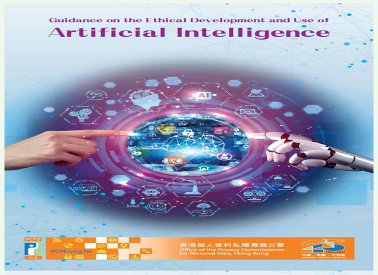
- To assist organisations that wish to apply DPbD when designing and building ICT systems
- To provide system architects and software developers with DPbD principles and good data protection practices

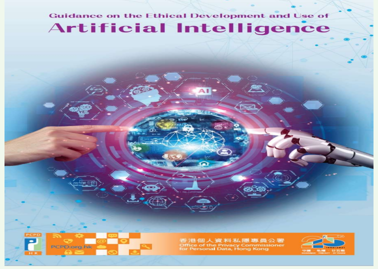
GUIDE TO
DATA PROTECTION
BY DESIGN
FOR ICT SYSTEMS

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

香港個人資料私隱專員公署 Privacy Commissioner for Personal Data, Hong Kong

Guidance on the Ethical Development and Use of Artificial Intelligence


Guidance on the Ethical Development and Use of Artificial Intelligence


Guidance on the Ethical Development and Use of Artificial Intelligence

Guide to Data Protection by Design for ICT Systems

GUIDE TO
DATA PROTECTION
BY DESIGN
FOR ICT SYSTEMS

Thank you!

Telephone ：	2827 2827
Website ：	www.pcpd.org.hk
Email ：	communications@pcpd.org.hk