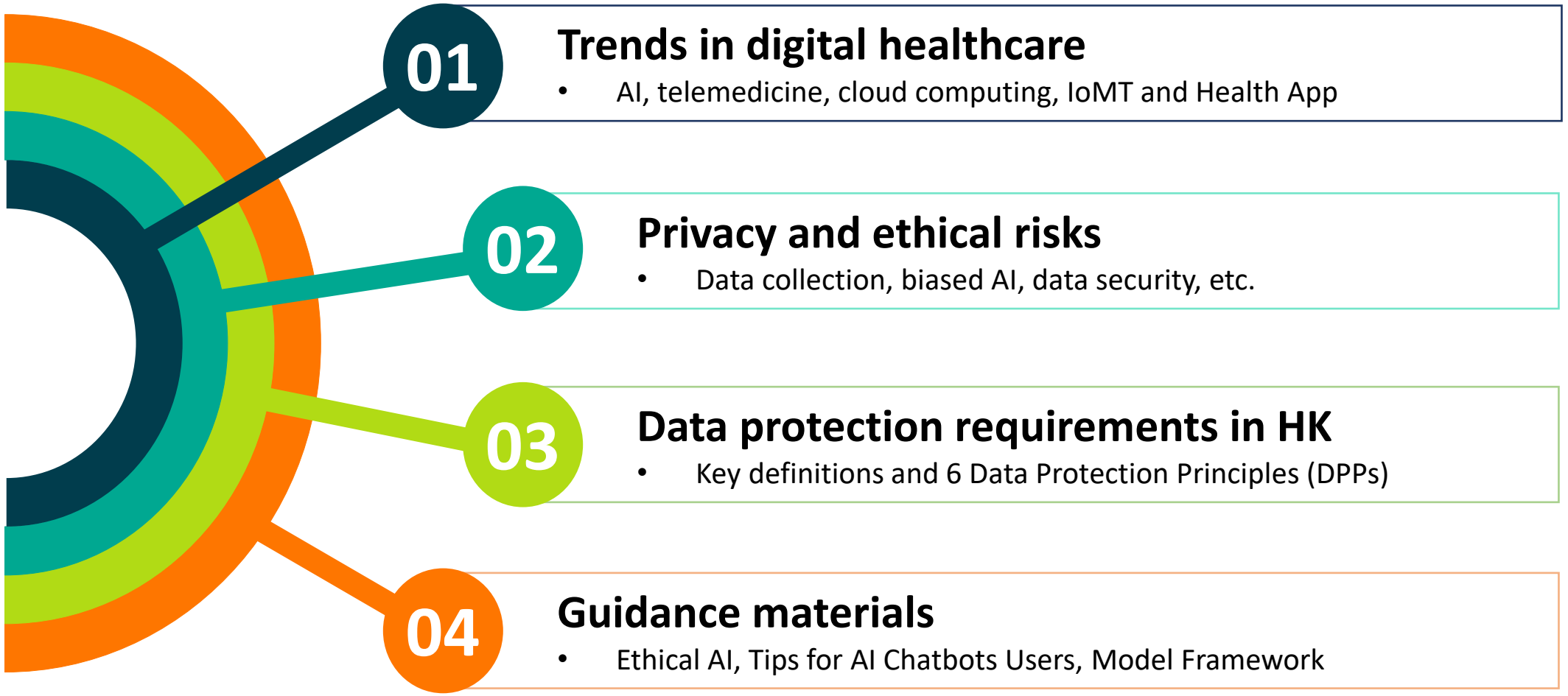
BMEG3103 Big Data in HealthCare
24 October 2024

Privacy and Data Security in Digital Healthcare Environment

Joyce Liu
Ag. Senior Legal Counsel &
Head of Global Affairs & Research
Office of the Privacy Commissioner for Personal Data

Outline

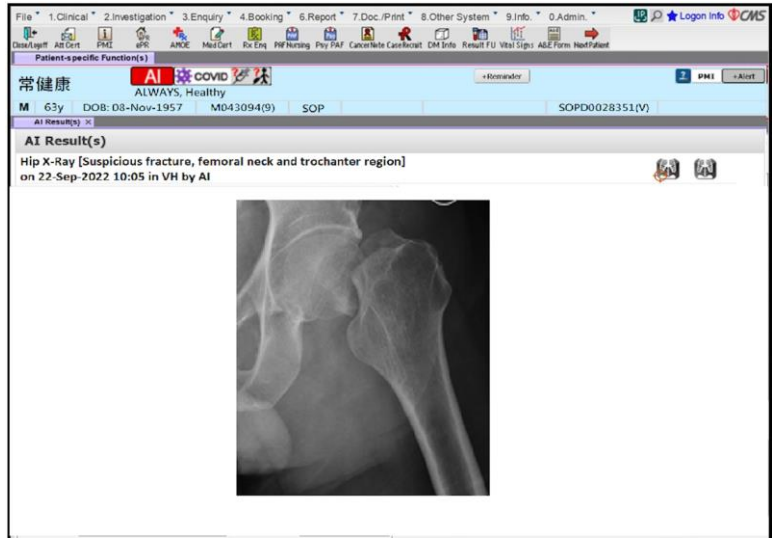

01
Trends in digital healthcare
• AI, telemedicine, cloud computing, IoMT and Health App
02
Privacy and ethical risks
• Data collection, biased AI, data security, etc.
03
Data protection requirements in HK
• Key definitions and 6 Data Protection Principles (DPPs)
04
Guidance materials
• Ethical AI, Tips for AI Chatbots Users, Model Framework

01 Trends in digital healthcare

Healthcare and AI

Artificial Intelligence (AI)

- A family of technologies that **mimic human intelligence and involve the use of computer programmes and machines to perform or automate tasks**
- Benefits of applying AI in medicine (Venture Beat, 2022):
  - Enable **accurate and early diagnosis**
    - AI algorithms can extract valuable insights from vast amount of data readings
    - AI technology can identify small details with more precision than humans
  - Can **handle repetitive tasks automatically and tirelessly**



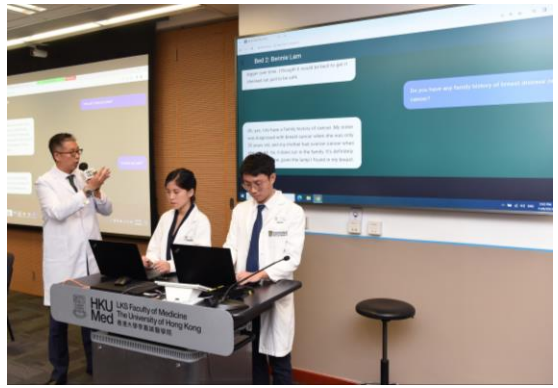
(Source: HKEJ, 2022)

In HK, the Hospital Authority (HA) cooperated with local universities to develop an AI tool for hip fracture detection. 1 million x-ray films from HA's database were used to train the AI model.

Application of AI

(Source: Microsoft, 2023)

Microsoft introduced an automated clinical documentation application which generates notes based on the conversations during patient visits using GPT-4.



(Source: HKU, 2023)

HKU developed a diagnostic application, "AI virtual patient" for training medical students, allowing them to virtually simulate interactions with patients during bedside consultations.

This Just In...

(Source: CUHK, 2024)

CU Medicine pioneers the introduction of a novel AI system for detection of early gastric cancers during upper GI endoscopy to increase the detection rate of the disease and facilitate endoscopists' training

21 October 2024

The Chinese University of Hong Kong's (CUHK) Faculty of Medicine (CU Medicine) recently became the foothold of the world's first centre to test a novel AI-powered upper gastrointestinal endoscopy system for the detection of gastric cancers. Given the success of AI-assisted colonoscopy, the team believes that the new technology will enhance the accuracy of detecting early gastric cancers and train endoscopists.

CU Medicine has engaged in clinical research in endoscopic and laparoscopic devices since the 1980s and translated novel endoscopic devices and technologies from bench to bedside. It introduced AI-powered colonoscopy detection as early as 2021. Studies proved that the technology not only contributed to a 40% increase in the adenoma detection rate but also improved the training of less experienced physicians.

Mobile App Empowered by AI

(Source: CUHK, 2024)

CUHK developed a depression assessment mobile app which uses AI to analyse the user's multimodal data, including facial expressions, voice, language and subjective mood state, as well as rest-activity statistics, to assist in diagnosing depression.

(Source: HKU, 2024)

HKU developed an AI-powered software that can turn smartphones into stethoscopes. It uses AI to measure heart sounds from the chest and conduct an analysis of whether the user could suffer from heart disease.

Telemedicine

Telemedicine

- The **practice of medicine over a distance**, in which interventions, diagnoses, therapeutic decisions, and treatment recommendations are based on patient data, documents and other information transmitted through **telecommunication** systems (World Medical Association, 2018)
- Gained popularity worldwide since the COVID-19 pandemic. Benefits include:
  - **Reducing physical contact**
  - **Alleviating crowdedness** in hospitals and clinics
  - **Easily accessible** and **cost-effective**

The Hospital Authority (HA) has launched the TeleHealth pilot programme through "HA GO" mobile app.

(Source: HA)

The CUHK Medical Centre also provides telemedicine service.

(Source: CUHKMC)

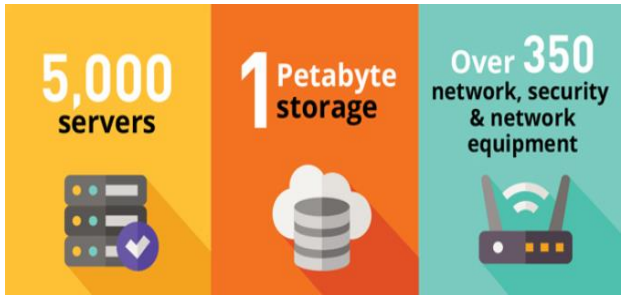
Cloud computing

Cloud computing

- Cloud computing offers a **centralised offsite storage** system
- Benefits (Forbes Advisor, 2022):
  - **Cost-efficient**
    - Reduce the need for maintaining costly IT infrastructure
  - Enable **flexible** subscription
    - Unlike a physical machine, a cloud storage system can be scaled up and down flexibly
  - Facilitate **big data analytics**
    - Due to the large sets of data available

During the COVID-19 pandemic, the US Centers for Disease Control and Prevention (CDC) processed millions of vaccination orders and manage contact tracing data with cloud services.

(Source: CDC, 2023)



The Singapore government has launched the "Healthcare-Cloud" to support the operation of 9 public hospitals. The H-Cloud is expected to help reduce 55% of operational costs by 2025.

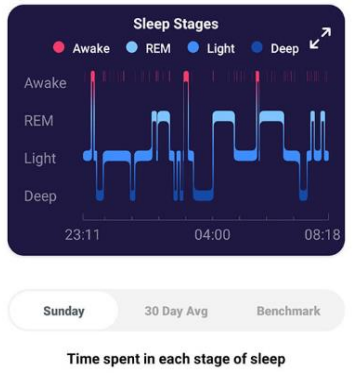
(Source: Ihis, 2022)

Internet of Medical Things

Internet of Medical Things (IoMT)

- **Connection of medical devices to networks** and the **sharing of data with healthcare applications** via Wi-Fi, Bluetooth, and radio-frequency identification (RFID) (Deloitte, 2022)
- **Improve patients' health outcomes**
  - Track patients' compliance with physicians' orders
  - Allow healthcare staff to access real-time data and make informed decision of treatment options (Digital Health, 2021)
- **Improve** the **management of patients and assets in healthcare facilities**
  - Allow healthcare staff to locate patients and available medical equipment in the healthcare premises (Mapsted, 2024)

A wearable that reminds patients to take medications.

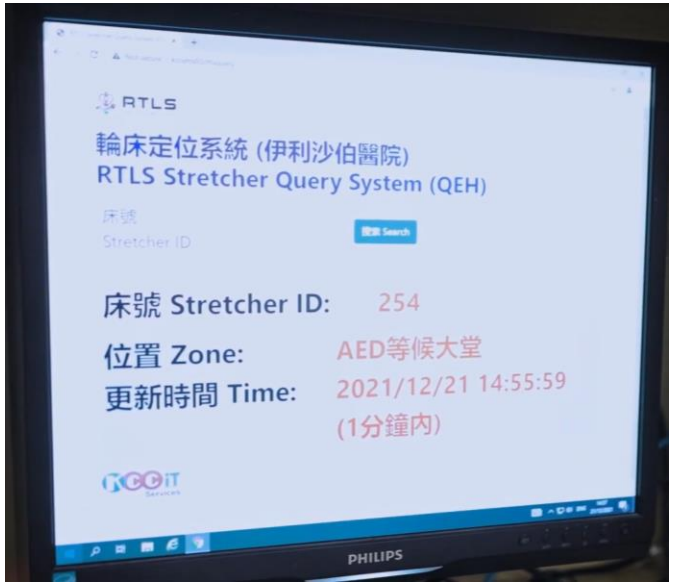


A sleep tracker.

Internet of Medical Things

HA is introducing the use of RFID straps across all 18 Accident and Emergency departments in public hospitals to enhance patient safety. If a high-risk patient wearing the strap attempts to leave the A&E department, an alarm will be triggered to alert the staff.

(Source: HA, 2024)



Queen Elizabeth Hospital has been employing a real time location system to track the location of stretchers for easy management and allocation.

(Source: HA, 2023)

Health and Wellness App

Health and Wellness App

- Different healthcare services are available in these apps, e.g. (KBI, 2021; Jellyvision, 2022):
  - Health screening and monitoring
  - Stress management
  - Provision of personalised health advice
- Number of health apps and usage:
  - As of Q2 2024, over 35,000 health apps are available on Apple App Store and Google Play Store respectively (Statista, 2024)
  - In 2023, there were 311 million health app users (Business of Apps, 2024)

***Pokémon Sleep**, a mobile game that functions as a sleep-tracker.*

***Blua Health**, a health app launched by Bupa, incorporates AI to analyze users' health via facial screening.*

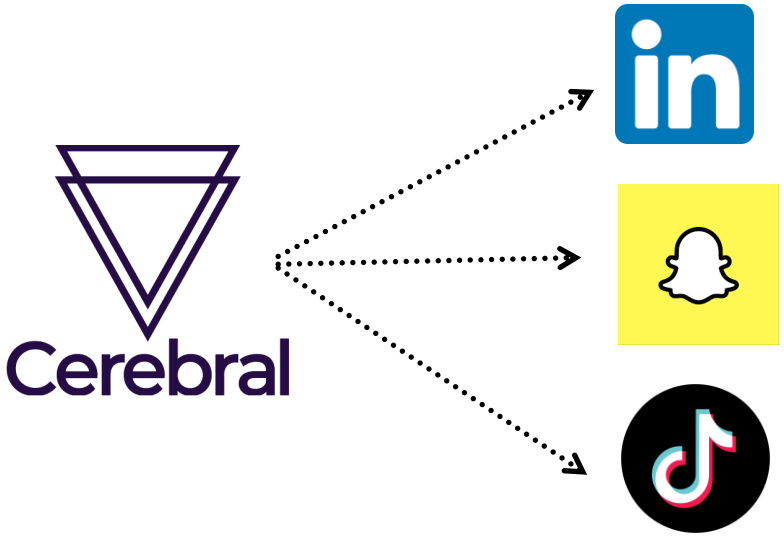
02 Privacy and ethical risks

Privacy and ethical risks

1) Collection and 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

- In a study of 20,991 health apps (BMJ, 2021):
  - **88%** of the apps can **collect** and **potentially share** user data
  - **56%** of data transmissions go to 3rd parties which include **adverts**, **analytics** and **other services**



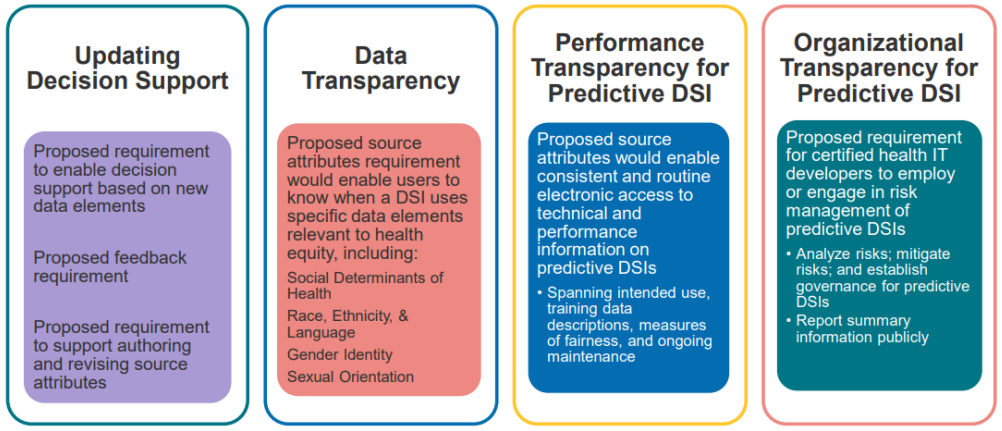
*In Apr 2024, US Federal Trade Commission proposed a **$7 million** penalty on online mental health services provider Cerebral for violating 3.2 million customers' privacy by **revealing their sensitive mental health conditions to third parties for advertising purposes**.*

(Source: FTC, 2024)

Privacy and ethical risks

2) Lack of transparency

- AI algorithms sometimes evolve beyond our comprehension
- Data processing and decision-making may take place in a "**black-box**"
- In March 2024, a rule released by the US Department of Health and Human Services became effective. One of its aims is to **enhance algorithmic transparency**: AI-driven applications are required to let the users **review the supporting evidence for unbiased decision-making**



(Source: ONC, 2023)

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 landmark study on an algorithm used widely by U.S. hospitals found out (Science, 2019):
  - **Dark-skinned** people were **less likely** to be referred to personalised care programmes
  - 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

3b) Bias and discrimination — Skewed data

- AI systems rely on **training data** to acquire their "intelligence"
- If training datasets are **skewed** and **dominated** by a particular group, AI systems may be **unreliable**, esp. when applied to **minorities**

- In a study of an AI model designed for predicting patients' loss of kidney function (STAT, 2020):
  - Only **6%** of the training data were from **female** patients
  - The **model performed worse** when tested on women—the **under-represented** group

(Source: STAT, 2020)

Privacy and ethical risks

4) Security of health data

- Health data is "going online", esp. with the wide adoption of telemedicine and cloud computing
- Health data stored online may fall prey to hackers
- Among all industries in Australia and UK, the **healthcare sector** accounts for the **largest proportion of data breach incidents**

Number of data breach incidents reported in Australia (by sector, top5) in 2024 (Q1-Q2)

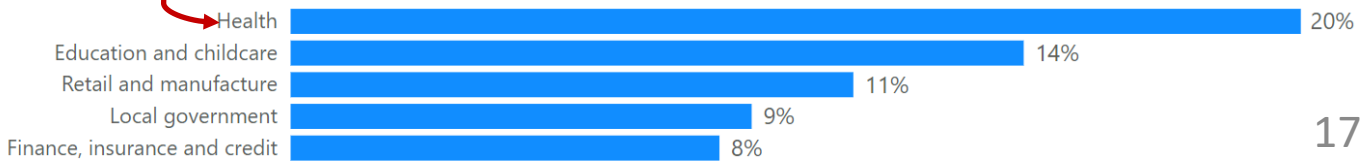
#1: Health (19%)

Sector	Number of notifications	Percentage of all notifications received
Health service providers	102	19%
Australian Government	63	12%
Finance (incl. superannuation)	58	11%
Education	44	8%
Retail	29	6%

(Source: OAIC, 2024)

Proportion of data breach incidents reported in UK (by sector, top 5) in 2024 (Q1-Q2)

#1: Health (20%)



(Source: UKICO, 2024)

Privacy and ethical risks

4) Security of health data

- Data Breach Incidents, if found to have been caused by inadequate security measures or other violations of the General Data Protection Regulation (GDPR), may result in **sanctions** by Data Protection Authorities (DPAs)

THE IRISH TIMES

Data & Security

Centric Health fined €460,000 over 2019 ransomware attack

Attack compromised data of about 70,000 Centric patients

Expand

Centric Health was hit by a ransomware attack in 2019.

Ciara O'Brien
Fri Feb 24 2023 - 14:12

Centric Healthcare has been fined €460,000 by the Data Protection Commissioner over a ransomware attack in 2019 that saw patient data encrypted by hackers.

The attack, which restricted access to patient data, hit 11 Primacare GP practices, which Centric Health acquired in 2016. At the time, the practices were being integrated into Centric Health's IT system.

The attack affected the data of 70,000 patients. Of those, 2,500 had their data deleted with no backup available during attempts to mitigate the attack.

Dublin-headquartered Centric offers GP, specialist care and dental services, to more than 400,000 patients throughout the State.

BLEEPINGCOMPUTER

NEWS | DOWNLOADS | VPNS | VIRUS REMOVAL GUIDES | TUTORIALS

Medical software firm fined €1.5M for leaking data of 490k patients

By Bill Toulas — April 28, 2022 — 12:17 PM — 1

The French data protection authority (CNIL) fined medical software vendor Dedalus Biology with EUR 1.5 million for violating three articles of the GDPR (General Data Protection Regulation).

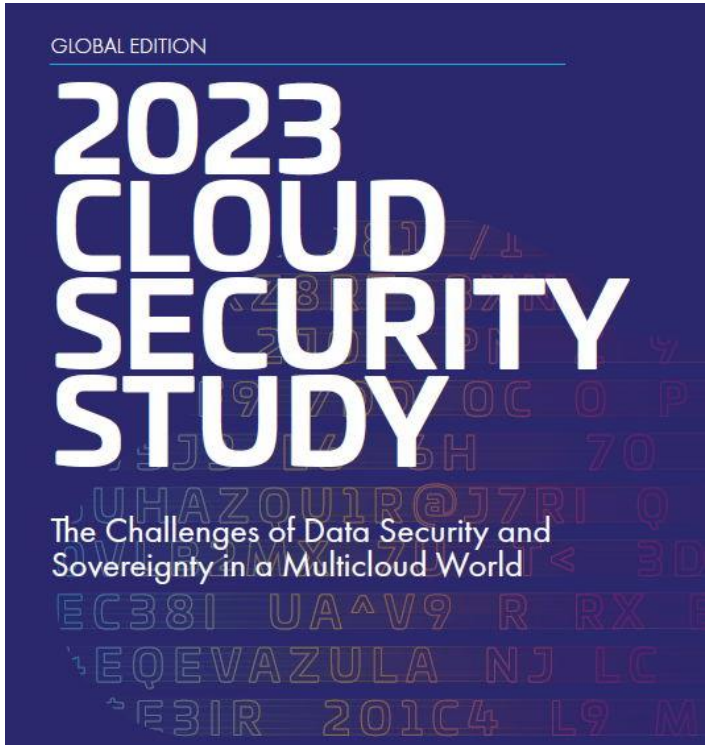
Dedalus Biology provides services to thousands of medical laboratories in the country and the fine is for exposing sensitive details of of 491,939 patients from 28 laboratories.

Privacy and ethical risks

5) Loss of control due to outsourcing

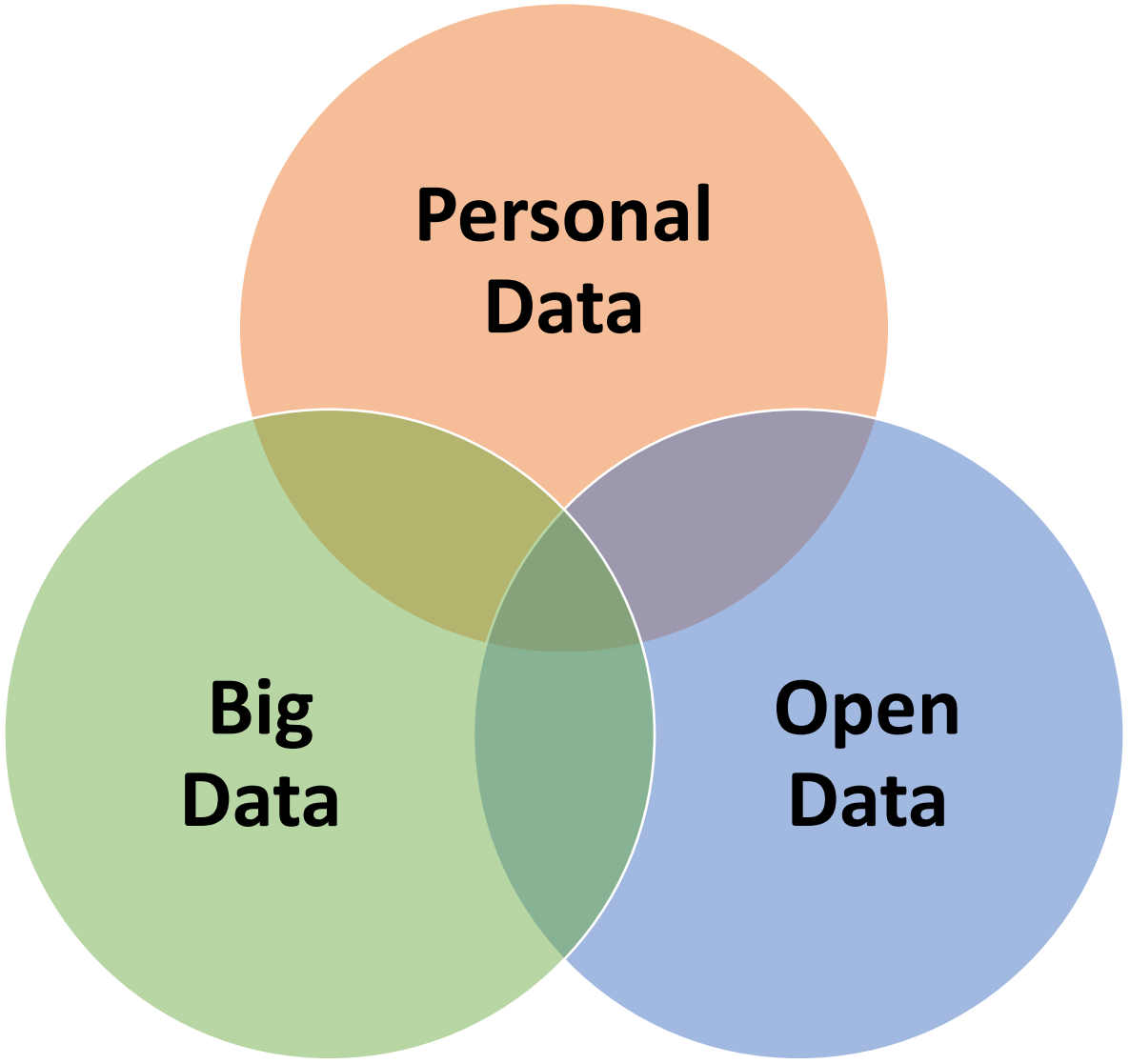
- Technical support services are often **outsourced** to boost efficiency. Examples of outsourcing include:
  - Saving patients' health data to **cloud storage**
  - Providing telemedicine consultations via **videoconferencing apps**

- In a survey of nearly 3,000 IT and security professionals across 18 countries (Thales, 2023):
  - 39% of businesses have experienced a data breach in their cloud environment last year



(Source: Thales, 2023)

03 Data protection requirements in Hong Kong


Personal Data
Big Data
Open Data

What is personal data?

According to **Section 2(1) of the Personal Data (Privacy) Ordinance**, personal data means any data —

- Relating directly or indirectly to a **living individual**;
- Practicable for the **identity** of the individual to be directly or indirectly **ascertained**; and
- In a form in which **access to or processing of is practicable**

Pop Quiz:

Which one of the following is personal data?

A. Covid-19 vaccination certificate 

B. Bank statements 

C. Octopus Card number 

D. Joyce's mobile number 

Who are involved?

Personal Data (Privacy) Ordinance:

Data subject	Data user	Data processor
The individual who is the **subject** of the data	A person who, either alone or jointly or in common with other persons, controls the **collection**, **holding**, **processing** or **use** of the data;	A person who – a) Processes personal data **on behalf of another person**; and b) Does **not** process the data for any of his/her **own purposes**

General requirements of personal data protection

6 Data Protection Principles (DPPs):

- Represent the core requirements of the Personal Data (Privacy) Ordinance (PDPO)
- Cover the **entire lifecycle** of personal data, from **collection**, **holding**, **processing**, **use** to **deletion**
- Data users must comply with the 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 practicable 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.

DPP1—Purpose and manner of collection of personal data

Example of 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

What should be done?

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, etc

Example from "Application of Generative AI":

> *"Microsoft introduced an automated clinical documentation application which generates notes based on the conversations during patient visits using GPT-4.*

If it involves recording the conversations, which probably include the personal data of patients, the patients should be notified beforehand.

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

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

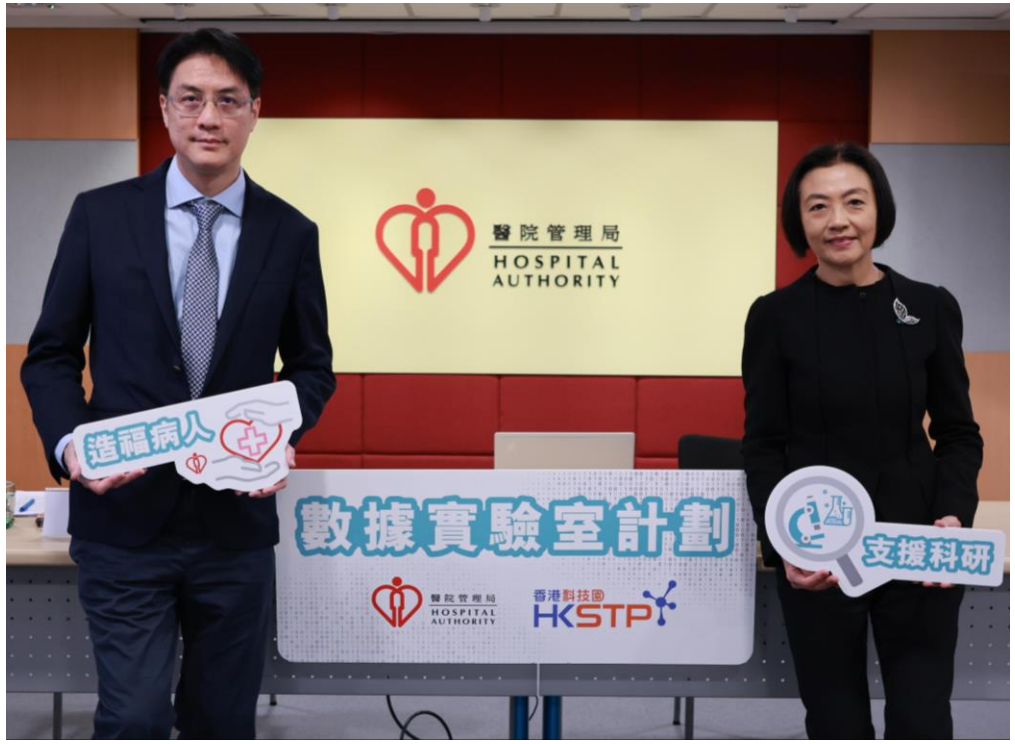
- Under certain circumstances, a relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using the data subject's personal data for a new purpose.

DPP3—Use of personal data

- However, under section 62 "Statistics and research" of the PD(P)O, personal data is exempt from the provisions of DPP3 where —
  - (a) The data is to be used for preparing statistics or carrying out research;
  - (b) The data is not to be used for any other purpose; and
  - (c) The resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them

醫院管理局與科技園正式開放數據平台支援科學園創科企業進行科研

(28 March 2024)



……醫管局與科技園公司公布，雙方於香港科學園內設置的「數據實驗室」正式開放給科學園內合資格的創科企業，申請使用醫管局的醫療數據作科研及開發用途……

……醫管局已在可供查閱的數據中，刪去可辨認病人身分的資料。數據並不會離開醫管局，無法下載、複製或存取。……

(Source: GovHK, 2024)

Pop Quiz:

Would section 62 exemption apply in this case?

Yes　No

Tips:

1. Is the data to be used for preparing statistics or carrying out research?
2. What is personal data? Are these information personal data?

DPP4—Security of personal data

- Data users should take all practicable steps to ensure the personal data that they hold is protected against unauthorised 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 unauthorised accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing

DPP4—Security of personal data

Practicable steps

Data users should consider:

1) the kind of data and the harm that could result from data security incidents;
2) the 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.

Examples of data breaches which involved loss of patient data for research purpose

瑪麗醫院醫生手提電腦懷疑失竊　載有360名外科病人資料

社會 20:23 2019/09/12

關注文章 儲存文章 分享:

熱門 流感通歌大全 下流上車族 兒童疫苗 季前發 梨泰院人踩人 李敏言 超市大搜查 1萬消費券 親太安娥寫

▲ 瑪麗醫院一名醫生手提電腦疑遭竊，載有約360名病人資料。(資料圖片)

瑪麗醫院今（12日）表示，該院一名醫生擁有的手提電腦，於本周二（10日）存放於辦公室期間懷疑失竊。有關手提電腦設有密碼，主要用於臨床研究及數據分析用途，載有約360名病人的姓名、身份證號碼、年齡、性別及臨床資料，電腦亦同時載有一批早年已離世病人的資料。

懷疑失竊的辦公室範圍需以密碼進出，亦設有獨立門鎖。醫院已就事件報警，並翻查閉路電視片段展開調查。醫院已透過早期事故通報系統向醫院管理局總辦事處報告事件，並已通知個人資料私隱專員公署跟進。

TOPick向院方查詢，院方表示涉事病人為外科病人。醫院亦就事件向影響的病人致歉，將通知受影響病人解釋事件，預計將於下周內完成通知工作。院方稱，失竊事件沒有影響醫院的臨床服務，亦不會對有關病人的治療構成影響。

2016年9月4日 (日) 要聞港聞 兩岸國際 產經 娛樂 副刊 男極圈 體育 馬經 波經 社論專欄 慈善基金 昔日東方

港大醫學院 3600病人私隱恐外洩 上一則 下一則

港大醫學院 3600病人私隱恐外洩

香港大學醫學院有一部手提電腦不翼而飛，三千六百多名病人的私隱恐外洩。港大醫學院昨公布，遺失的電腦載有三千多名瑪麗醫院及東華醫院腎科病人資料，包括姓名、身份證號碼、電話號碼及診斷結果等，二千多人資料無被加密；而失竊的辦公室並無安裝閉路電視，港大已報警及通報私隱專員公署，日後會加強工作地點的防盜設施，暫無人被捕。

我的瀏覽記錄

事發於本月一日，內科學系位於瑪麗醫院新教授樓三樓的辦公室，有一部手提電腦懷疑被盜。經初步估計，事件涉及三千六百多名瑪麗醫院及東華醫院腎科病人的個人臨床資料，主要為化驗報告，還有病人的姓名、身份證號碼、部分病人的電話號碼、診斷和藥物等資料；當中九百零一名病人資料獲加密處理。手提電腦需輸入用戶名稱及密碼才能登入系統。

瑪麗醫院新教授樓辦公室有手提電腦失竊。（資料圖片）

辦公室沒裝天眼

港大醫學院指，職員當日上班時發現失竊，內科學系已即時要求職員重設系統密碼，並提醒所有職員嚴格遵守大學的系統安全及工作指引，並對部門內所有個人資料的儲存進行檢視，加強安全管理。部門會加強工作地點的防盜設施，避免失竊事件再次發生。學系將會通知相關的病人。

瑪麗醫院指辦公室內並沒有裝設閉路電視，大門的密碼門鎖於辦公時間後會被鎖上，保安人員於事發前一晚及當日凌晨巡查過有關地點，沒有發現任何異常情況，向醫院管理局總辦事處通報，瑪麗醫院亦會與醫學院保持密切聯繫，了解有關事件的處理進度。

私隱署循規審查

警方表示，當日接獲院校女職員報案，列作盜竊，由西區警區刑事調查三隊接手，暫無人被捕。私隱專員公署亦指已接獲通報，會展開循規審查。

港大醫學院腦內科學系教授張倩輝表示，昨日收到學系電郵，提醒職員小心處理病人資料。他又指，相信有關資料是臨床研究或實驗所用，職員把病人資料從主機轉至手提電腦或USB記憶棒時，一般會經過系統加密，即使裝置被盜或遺失亦要輸入密碼才可看到病人資料，但研究員分析資料途中未必會加密資料，令資料外洩機會較大。

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 the personal data is or is to be used.

DPP6—Access to personal data

Data subject's rights

- A data subject must be given access to his personal data and the right 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)

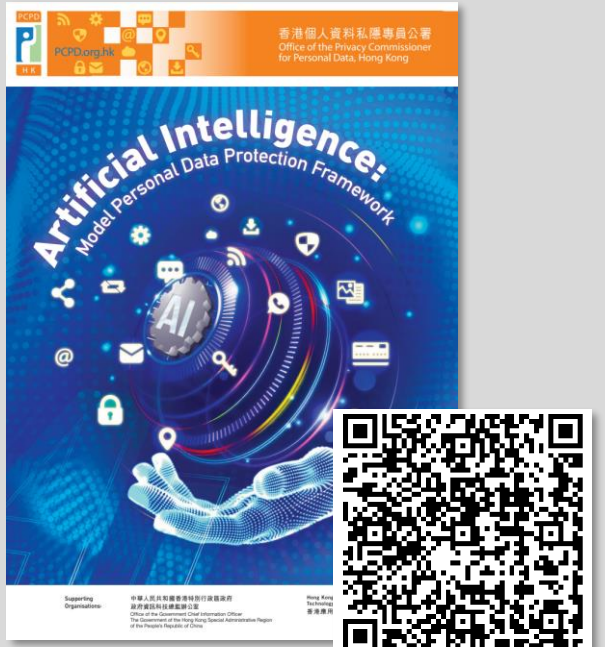
04 Guidance materials

PCPD's Guidance Materials on Artificial Intelligence

Guidance on the Ethical Development and Use of Artificial Intelligence (Aug 2021)

10 Tips for Users of AI Chatbots (Sep 2023)

Artificial Intelligence: Model Personal Data Protection Framework (Jun 2024)

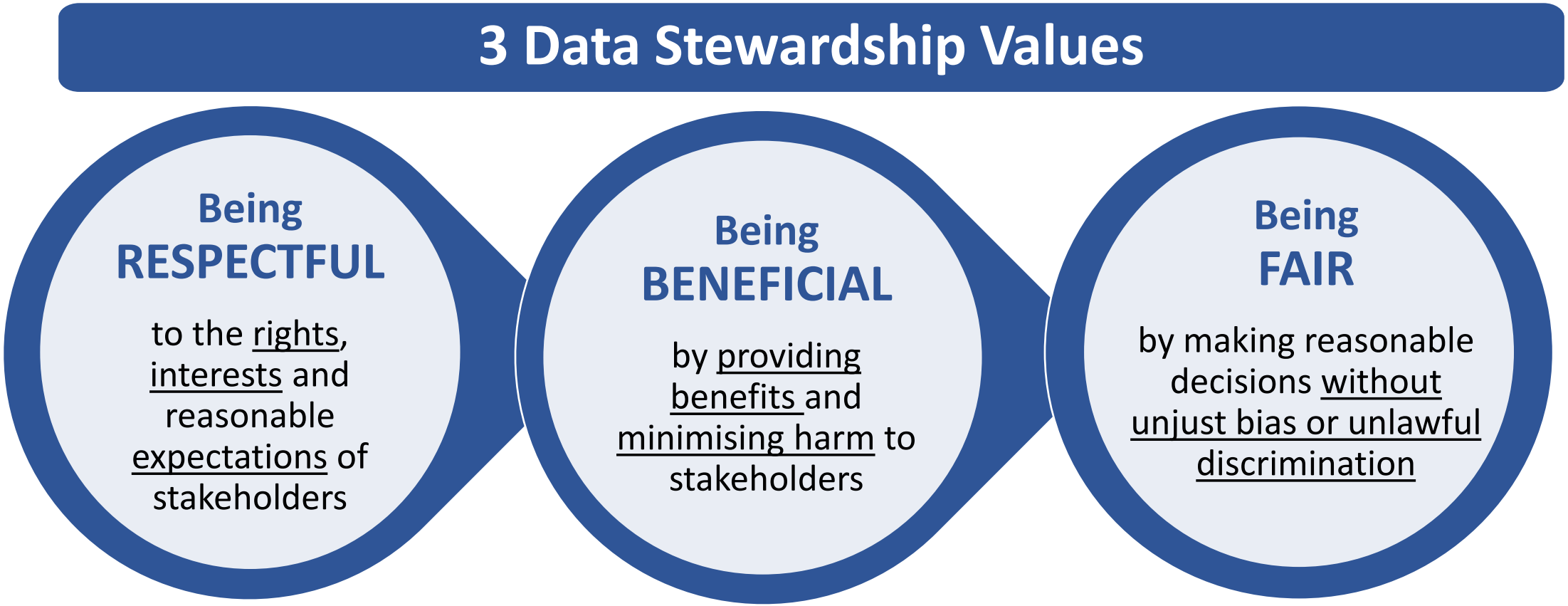


Guidance on the Ethical Development and Use of Artificial Intelligence

Objectives

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

Guidance on the Ethical Development and Use of Artificial Intelligence



Guidance on the Ethical Development and Use of Artificial Intelligence

7 Ethical Principles for AI

1. ACCOUNTABILITY

Organisations should:

- Be responsible for their actions
- Be able to provide sound justifications for the actions

2. HUMAN OVERSIGHT

The level of human involvement should:

- Be proportionate to the risks and impact of using AI

Guidance on the Ethical Development and Use of Artificial Intelligence

7 Ethical Principles for AI

3. TRANSPARENCY & INTERPRETABILITY

Organisations should:

- Disclose their use of AI and the relevant data privacy policies
- Improve the interpretability of automated decisions

4. DATA PRIVACY

Organisations should:

- Put effective data governance in place to protect personal data privacy

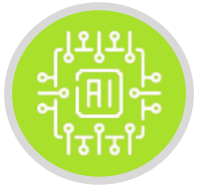
Guidance on the Ethical Development and Use of Artificial Intelligence

7 Ethical Principles for AI

5. FAIRNESS

Organisations should:

- Treat individuals in a reasonably equal manner, without unjust bias or unlawful discrimination



6. BENEFICIAL AI

The use of AI should:

- Provide benefits to stakeholders
- Minimise harm to stakeholders

7. RELIABILITY, ROBUSTNESS & SECURITY

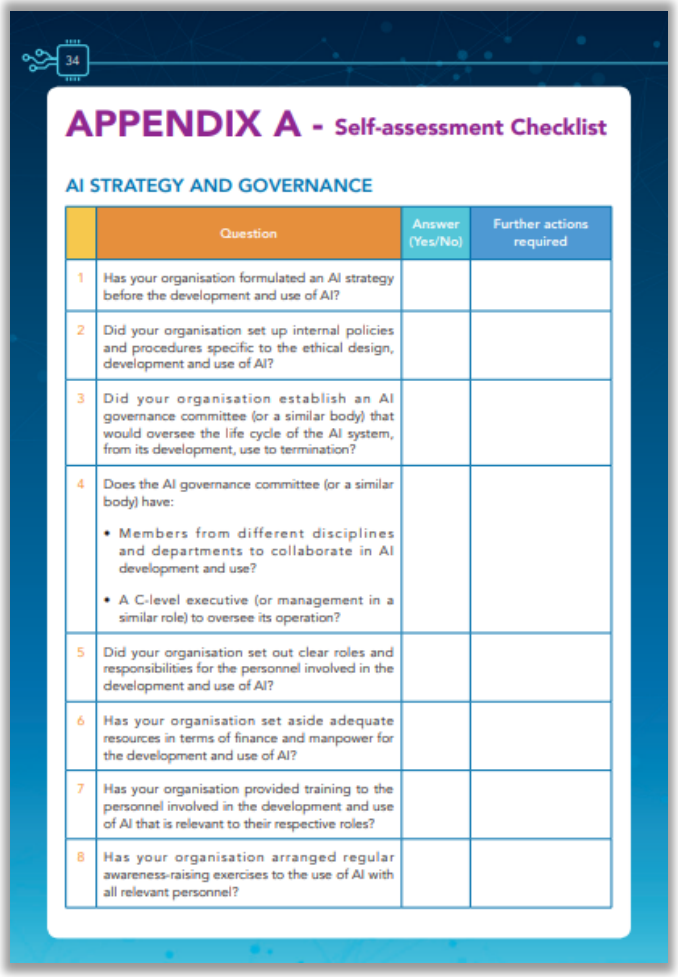
AI systems should:

- Operate reliably
- Be resilient to errors
- Be protected against attacks

Guidance on the Ethical Development and Use of Artificial Intelligence

Self-assessment Checklist

- The checklist contains **self-assessment questions** on the **4 major business processes**
- Practical suggestions made by the Guidance are also incorporated



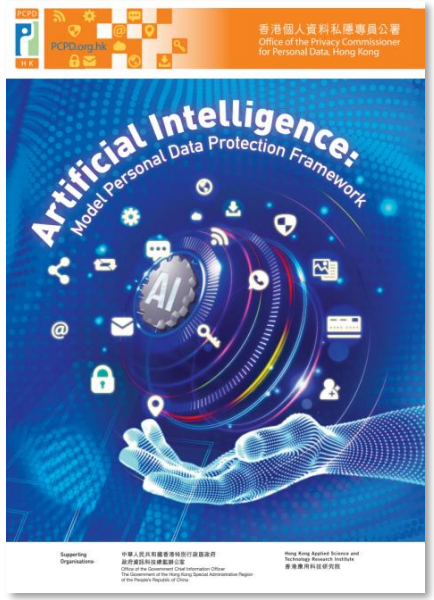
34

APPENDIX A - Self-assessment Checklist

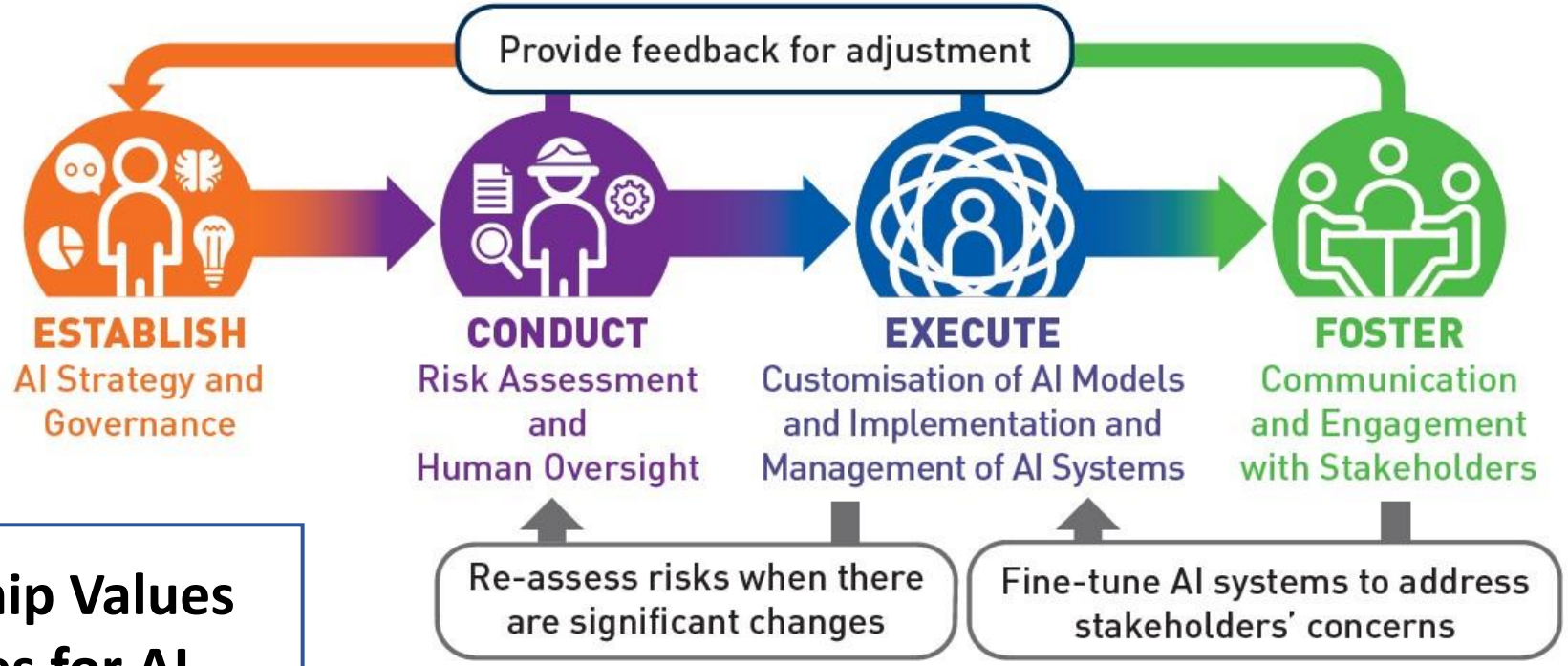
AI STRATEGY AND GOVERNANCE

	Question	Answer (Yes/No)	Further actions required
1	Has your organisation formulated an AI strategy before the development and use of AI?		
2	Did your organisation set up internal policies and procedures specific to the ethical design, development and use of AI?		
3	Did your organisation establish an AI governance committee (or a similar body) that would oversee the life cycle of the AI system, from its development, use to termination?		
4	Does the AI governance committee (or a similar body) have: • Members from different disciplines and departments to collaborate in AI development and use? • A C-level executive (or management in a similar role) to oversee its operation?		
5	Did your organisation set out clear roles and responsibilities for the personnel involved in the development and use of AI?		
6	Has your organisation set aside adequate resources in terms of finance and manpower for the development and use of AI?		
7	Has your organisation provided training to the personnel involved in the development and use of AI that is relevant to their respective roles?		
8	Has your organisation arranged regular awareness-raising exercises to the use of AI with all relevant personnel?		

Model Personal Data Protection Framework

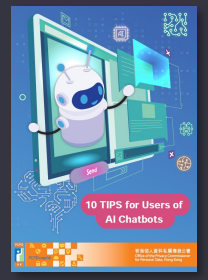


Assist Organisations to Procure, Implement and Use AI



Adheres to:

- 3 Data Stewardship Values
- 7 Ethical Principles for AI



10 Tips for Users of AI Chatbots

Before Registration / Use When Interacting with AI Chatbots Safe and Responsible Use of AI Chatbots

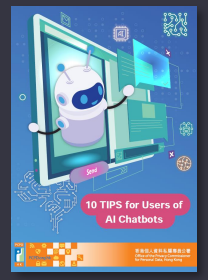
AI

A) Before Registration / Use:

1. **Read the Privacy Policy, the Terms of Use** and other relevant data handling policies

2. Beware of **fake apps** and **phishing websites** posing as known AI chatbots

3. Adjust the settings to **opt-out of sharing chat history** (if available)

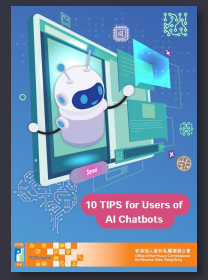


10 Tips for Users of AI Chatbots

AI

B) When Interacting with AI Chatbots:

4. **Refrain from sharing** your own **personal data** and others' personal data
5. Submit a **correction or removal request**, if necessary
6. Guard against **cybersecurity threats**
7. **Delete outdated conversations** from chat history



10 Tips for Users of AI Chatbots

Before Registration / Use When Interacting with AI Chatbots **Safe and Responsible Use of AI Chatbots**

AI

C) Safe and Responsible Use of AI Chatbots:

8. Be **cautious about using the information** provided by AI chatbots

9. **Refrain from sharing confidential information** and files

10. **Teachers / parents should provide guidance** to students when they are interacting with AI chatbots

Thank you!

www.pcpd.org.hk

communications@pcpd.org.hk

Please follow us!