Webinar on Cyber Security and Personal Data Privacy Protection in eHRSS
3 October 2023

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

01 WHAT IS HAPPENING

Smart Healthcare

Strategic goals

In the Hospital Authority Strategic Plan 2022-2027, four strategic goals are set as follows:

(a) provision of smart healthcare;

(b) development of smart hospitals;

(c) nurture of smart workforce; and

(d) enhancement of service supply.

TeleHealth

醫健通 ehealth

HA Go

Smart Healthcare

The Government of the Hong Kong Special Administrative Region
Press Releases

GovHK 香港政府一站通 繁體版 简体版

RSS | Font Size: A A

Secretary for Health visits Hospital Authority informa GO

Secretary for Health visits Hospital Authority information technology and innovation facilities (with photos)

****

The Secretary for Health, Professor Lo Chung-mau, visited information technology and innovation facilities of the Hospital Authority (HA) this afternoon (July 14) to get a better grasp of the latest progress of HA's work on facilitating the use of technology to enhance clinical and medical services.

Photo

Date: 14 July 2023

"Developing smart hospitals is a key strategy for the sustainable development of the public healthcare system. Healthcare staff can provide high quality services to patients with the aid of technology such as 5G remote diagnosis and treatment technology, and smart robots. These technologies can also alleviate, in the long run, the imbalance of manpower supply and service demands faced by the public healthcare system,"

Sharing of Medical Records

Promote eHealth

- ✓ Explore mandating the upload of more types of health records by legislation, with a view to further transforming eHealth into a key infrastructure integrating public and private healthcare systems.
- ✓ Consider the further implementation of cross-boundary use of electronic medical records-Pilot Scheme for Supporting Patients of Hospital Authority in Guangdong-Hong Kong-Macao Greater Bay Area – launched in May 2023

港聞 / 社會新聞

醫健通｜八成港人登記使用　醫衞局研究立法規定上載重要醫療紀錄

2018 年至 2022 年
已登記醫健通的市民人數
及其所佔該年齡群組的人口比例

	登記市民人數 (所佔年齡群組的人口比例)				
	2018 年	2019 年	2020 年	2021 年	2022 年
14 歲或以下	24 412 (2.9%)	43 343 (5.1%)	53 725 (6.5%)	88 095 (11.1%)	204 725 (27.2%)
15 至 64 歲	469 775 (8.8%)	607 032 (11.4%)	691 112 (13.3%)	3 492 060 (68.3%)	4 230 933 (84.4%)
65 歲或以上	424 790 (32.5%)	529 089 (38.9%)	608 880 (43.0%)	971 944 (65.0%)	1 295 960 (82.7%)
總數	918 977 (12.3%)	1 179 464 (15.7%)	1 353 717 (18.2%)	4 552 099 (61.5%)	5 731 618 (78.2%)

Source: 香港01, 12-7-2023

02 BENEFITS AND PRIVACY PITFALLS

Benefits vs Privacy Risks

- ✓ Optimize workflows, streamline processes
- ✓ Save time, save paper
- ✓ Reduce staff burnout
- ✓ Improve data flow and data management

- ✓ Reduce error rates, improve patient care
- ✓ Improve patient experience

AI, Machine Learning, Big Data

1) Collection & Use of Data

2) Lack of Transparency

3) Bias and Discrimination

4) Security of Health Data

5) Loss of Control due to Outsourcing

Guidance on the Ethical Development and Use of Artificial Intelligence

- Establish AI strategy and governance;
- Conduct risk assessment and human oversight;
- Execute development of AI models and management of overall AI Systems; and
- Foster communication and engagement with stakeholders.

Recent Notable Data Breach Incident

Sep 2023

【數碼港資料外洩】黑客暗網發放400GB洩取資料　數碼港CEO在內員工個人資料失守、孫東：指示各部門檢討

Hot Talk 13:53 2023/09/13

Source: 經濟日報, 13-9-2023

Aug 2022

Guidance Note on Data Security Measures for Information and Communications Technology

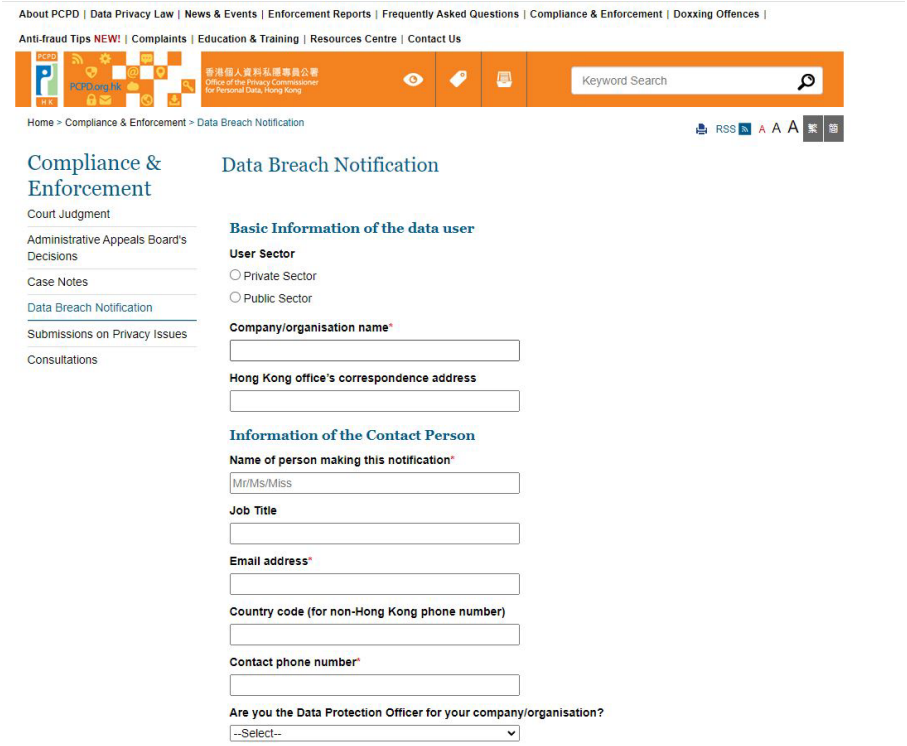
- Data Governance and Organisational Measures
- Risk Assessments on data security for new systems and applications
- Technical and Operational Security Measures
- Data Processor Management
- Remedial actions in the event of Data Security Incidents
- Regularly Monitoring, Evaluating and Improving compliance with data security policies
- Data Security Measures for Cloud Services, “Bring Your Own Devices” and Portable Storage Devices.

02 GETTING PREPARED

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

PREPARING FOR CONTINGENCY – DATA BREACH RESPONSE PLAN

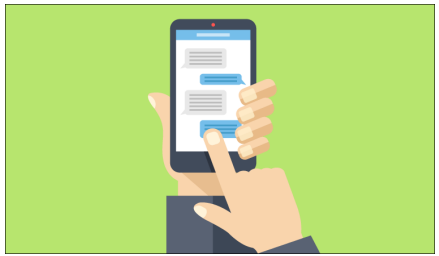
A data breach response plan is a document setting out how an organisation will respond in the event of a data breach. A comprehensive data breach response plan helps ensure a quick response to and effective management of a data breach. The plan should outline a set of procedures to be followed in the event of a data breach and the data user's strategy for identifying, containing, assessing and managing the impact brought about by the incident from start to finish. A prompt response to a data breach may substantially minimise and contain the impact of a breach.

The plan is recommended to cover the following aspects (non-exhaustive):

- A **description of what constitutes a data breach** with examples tailored to the nature of the organisation, and the criteria that trigger the implementation of the data breach response plan
- An **internal incident notification procedure** to escalate the breach to the senior management, the data protection officer and/or dedicated data breach response team, incorporating a standard form to facilitate the reporting of the required information
- A **contact list** with contact details of all breach response team members (e.g., the core management, chief data protection officer, information technology experts, risk management and human resources professionals)
- A **risk assessment workflow** to assess the likelihood and severity of the harm caused to the affected data subjects as a result of the breach
- A **containment strategy** for containing and remedying the breach
- A **communication plan** covering the criteria and threshold for determining whether the affected data subjects, regulatory authorities and other relevant parties should be notified; the kind of information that must be provided; the point of contact in the organisation responsible for liaising with the stakeholders; and the methods of notification
- An **investigation procedure** for investigating the breach and reporting the results to the senior management
- A **record-keeping policy** to ensure that the incident is properly documented as

Case Sharing (1)
Sending medical report by email without encryption

- The Complainant's son underwent a COVID-19 test at a hospital.
- When the complainant received his son's test report, he found that it was unencrypted.



Case Sharing (1)
Sending medical report by email without encryption

- 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, test reports contain sensitive personal data. Measures shall be taken to enhance the security of personal da contained in the test reports.

Thank you!

Telephone： 2827 2827

Website： www.pcpd.org.hk

Email： communications@pcpd.org.hk