Symposium on Cyber Security on Medical and Healthcare System

HKPC Building, Kowloon Tong 1 December 2017

Privacy Protection and Data Governance in the Internet of Medical Things

Stephen Kai-yi Wong, Barrister
Privacy Commissioner for Personal Data, Hong Kong

Presentation Outline

- Overview of the Personal Data (Privacy) Ordinance
- Privacy issues of IoMT and sensitive personal data
- Accountability – 'Privacy Management Programme'
- 'Privacy by Design' & 'Privacy Impact Assessment'
- Tips for senior management

Overview of the Personal Data (Privacy) Ordinance

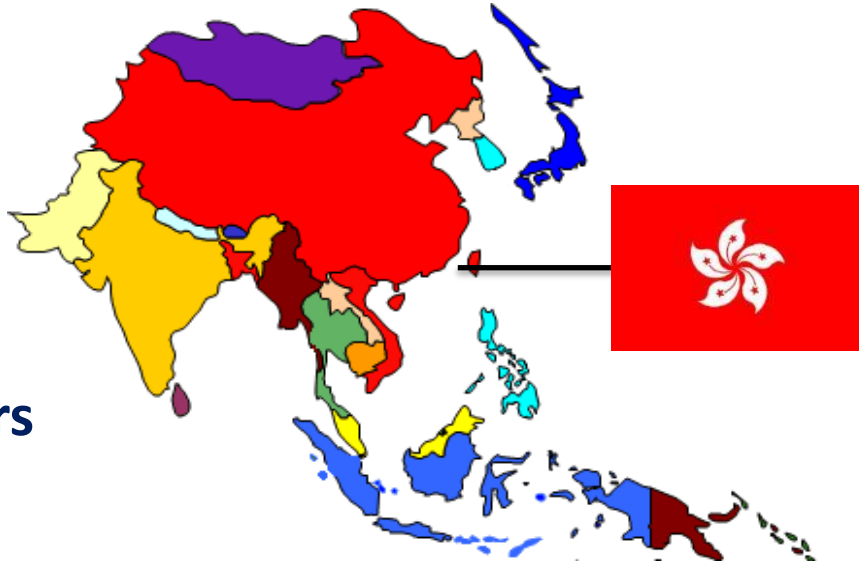
Personal Data (Privacy) Ordinance

- 1st comprehensive data protection law in Asia, enacted in 1995

- Referenced to 1980 OECD Privacy Guidelines and 1995 EU Data Protection Directive

- Covers the public (incl. the government) and private sectors

- Principle-based; technology neutral



Personal Data (Privacy) Ordinance

6 保障資料原則 Data Protection Principles

PCPD.org.hk

1 收集目的及方式 Collection Purpose & Means

資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

2 準確性、儲存及保留 Accuracy & Retention

資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的實際所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

3 使用 Use

個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

4 保安措施 Security

資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5 透明度 Openness

資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction

資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

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

Not only data security

- **Data security is only one part of personal data protection**

  We also need to consider:

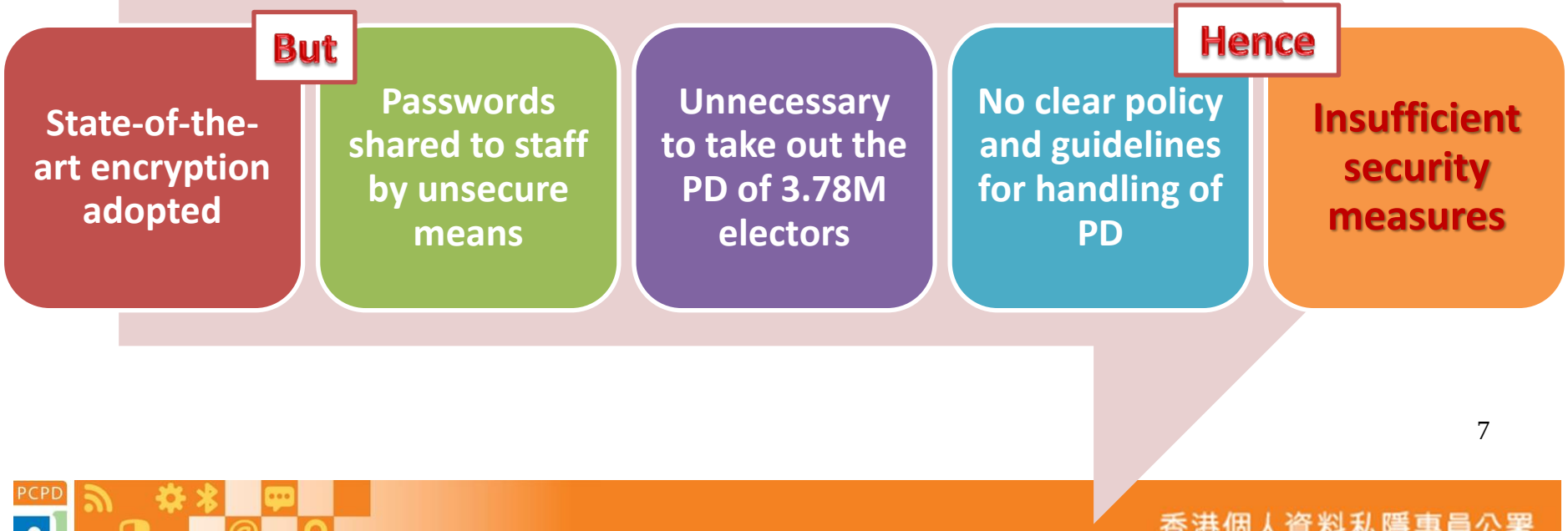
Data minimisation – collect only data that is necessary for the purpose

Purpose Limitation – use the data only for the original or directly related purpose

Transparency – to be open and honest to the public (data subjects) about data collection and how it will be handled

Not only technical security measures

- Organisational measures are also critical for data security
- Case sharing: REO lost 3.78M electors' personal data during 2017 CE Election



Privacy Issues of IoMT & Sensitive Personal Data

IoT / IoMT

- **Healthcare Internet of Things (IoT) or "Internet of Medical Things" (IoMT):**

  An interconnected infrastructure of medical devices and software applications that can communicate with other healthcare systems.

- **From large-scale healthcare systems and medical software, to consumer wearable devices,**
  e.g. fitness bands/ heartrate monitors/ bloody-sugar monitors

IoT / IoMT

- **Potential benefits in improved medical care and health services: – real time monitoring; more accurate data; speedy response.**

- **Need to strike a balance – a risk-based approach with due regard to the sensitivity of the data, and the potential harm if the data is mishandled**

Privacy Concerns & Data Security

- Processing power and sophistication of IoMT devices – collects and processes enormous amount of person data on physiology and medical status, perhaps also the location!

- Nature of the data collected:

  - Sensitive personal data
    (e.g. ID number; genetic information; medical condition & illnesses)

  - General data which, upon processing or analysis, may reveal or imply sensitive information about that person (e.g. sexuality; psychiatric or psychological conditions)

Privacy Concerns & Data Security

- Data in IoMT are not merely stored in the computer of 1 clinic – 'interconnectivity' means the entire dataset is at risk of unauthorised activities.

- A 'honey pot' of data – a treasure trove of sensitive data which can be an attractive and easy target
  - Interconnectivity - rather than a closed system - makes it vulnerable
  - Highly profitable to cyber criminals
  - Yet hitherto less well-guarded in its cybersecurity

- Must avoid becoming a lucrative and easy target for cybercriminals

Data security threats in HK

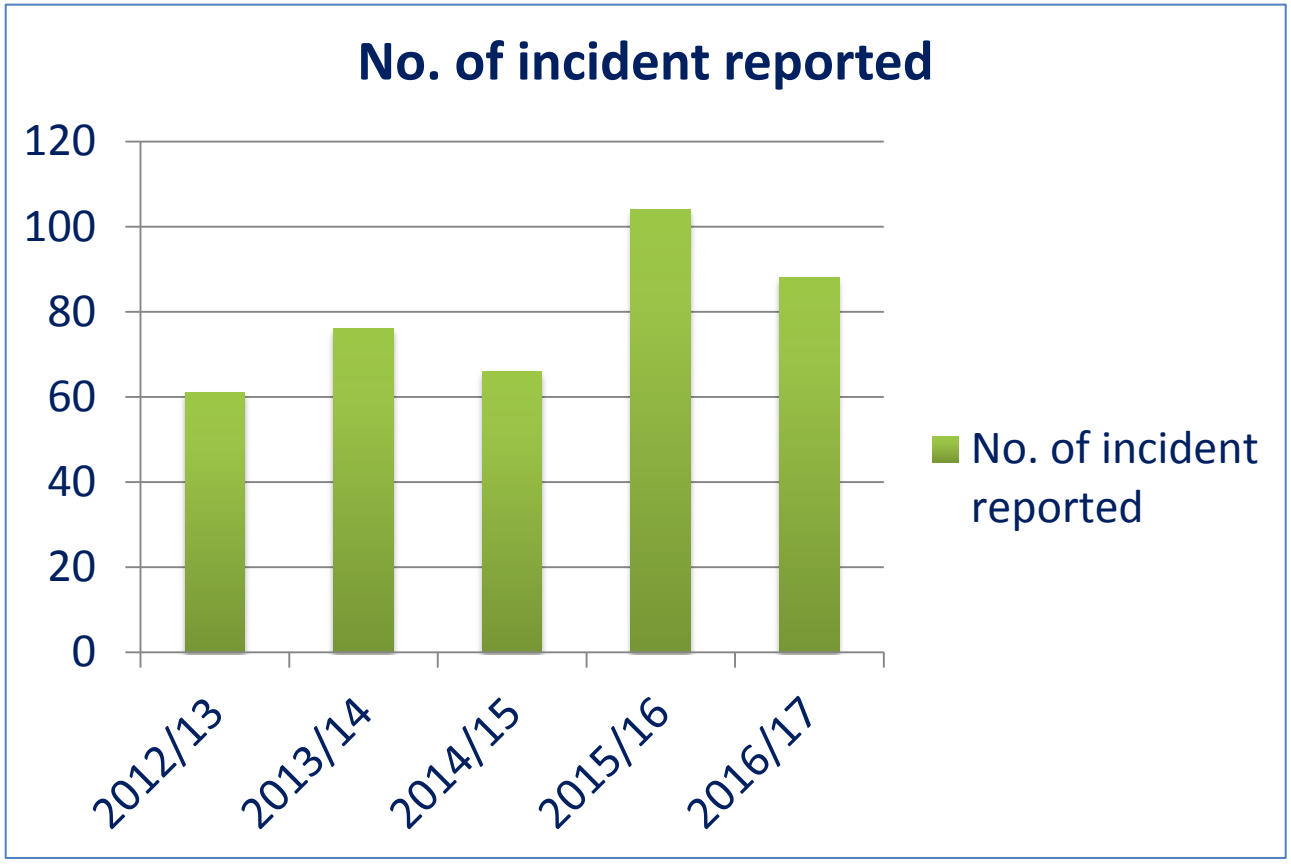
Telstra Cybersecurity Report (2017):
HK faces the 2nd-highest risk of cybersecurity attacks in Asia, in spite of a sharp increase in spending on IT Security

HK Computer Emergency Response Team (HKCERT) (2016): Received a 5-fold increase in cybersecurity incident reports in 2016 compared with 2010; cases of ransomware recorded a sharp increase since 2015

PwC survey (2016): Chinese companies had over 900% increase in cybersecurity incidents in 2 years since 2014

KPMG & HKICS survey (2017): cybersecurity now the Top 5 risks

Data breaches in HK



Year	No. of individuals affected
2012/13	17,451
2013/14	114,275
2014/15	77,409
2015/16	854,476
2016/17	3,859,338

Accountability –
Privacy Management Programme

Accountability - data protection as part of corporate governance

- Privacy Management Programme launched in 2014
- Encourages organisations to embrace personal data privacy protection as part of their corporate governance responsibilities
- Apply as a top-down business imperative throughout the organisation
- Have in place appropriate policies and procedures that promote good practices

From Compliance to Accountability

Compliance approach

- passive
- reactive
- remedial
- problem-based
- handled by compliance team
- minimum legal requirement
- bottom-up

Accountability approach

- active
- proactive
- preventative
- based on customer expectation
- directed by top-management
- reputation building
- top-down

PMP Best Practice Guide - Fundamental Principles

3 Top-down Management Commitments

1. Top-management commitment and buy-in
2. Setting up of a dedicated data protection office or officer
3. Establishing reporting and oversight mechanism

PMP Best Practice Guide - Fundamental Principles

7 Practical Programme Controls

1. Record and maintain **personal data inventory**
2. Establish and maintain data protection and **privacy policies**
3. Develop **risk assessment** tools (e.g. privacy impact assessment)
4. Develop and maintain **training plan** for all relevant staff
5. Establish workable **breach handling** and notification procedures
6. Establish and monitor **data processor** engagement mechanism
7. Establish **communication** so that policies and practice are made known to all stakeholders

PMP Best Practice Guide - Fundamental Principles

Two Review Processes

1

Develop an oversight review plan to check for compliance and effectiveness of the privacy management programme

2

Execute the oversight review plan making sure that any recommendations are followed through

Privacy by Design &
Privacy Impact Assessment

Privacy by Design

- An approach to systems engineering which takes privacy into account from the early stage of the design of a project
- To embed data protection controls as the default across the entire information life cycle
- An approach to data protection which is **preventive and proactive** - rather than remedial and reactive
- Adopted in 2010 by the global community of Data Protection Authorities – recognising Privacy by Design as an essential component of fundamental privacy protection

Privacy Impact Assessment

- PCPD has published a guidance on PIA
- The PIA includes 4 key components:

1. Data processing cycle analysis

- examines the purpose and rationale behind the project, incl. whether it is *necessary* to collect the *kind* and *amount* of personal data contemplated

- analyse the data processing cycle from collection to transmission, storage, access, use and destruction, preferably with the aid of annotated flow charts

Privacy Impact Assessment

- **The PIA includes 4 key components:**

2. Privacy risks analysis

- identify key privacy concerns and address them

- security measures should be commensurate with the privacy intrusiveness of the data processing

Privacy Impact Assessment

- The PIA includes 4 key components:

3. Avoiding or mitigating privacy risks

- risks should be avoided or mitigated to protect data from unauthorised access, use, disclosure or loss

- for data security: measures may include 2-factor authentication, encryption and back-ups

- for other privacy risks: measures may include avoid collecting sensitive data, or reducing the data retention period

Privacy Impact Assessment

- **The PIA includes 4 key components:**

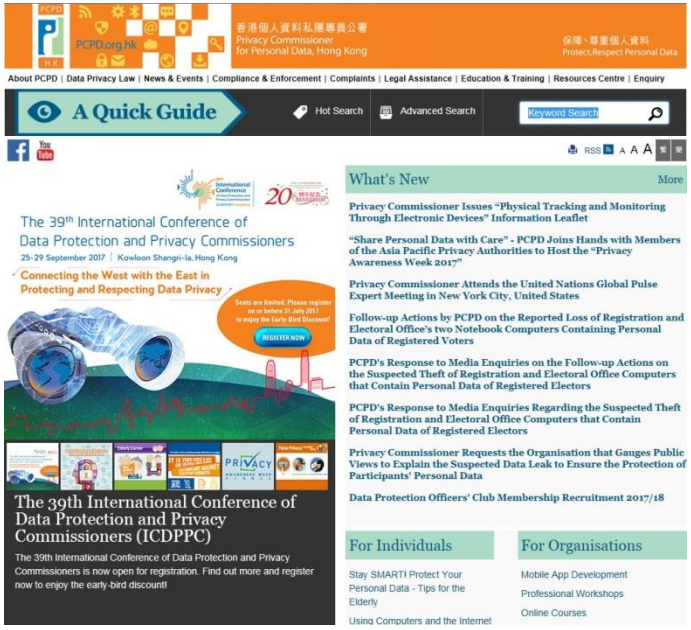
4. PIA reporting

- **the assessment findings and measures considered should be documented**

Tips for Senior Management on Data Governance

- Secure the buy-in from **top-management**
- Build a **culture** within organisation to protect privacy
- Keep abreast of **new developments** (PCPD's online resources, Data Protection Officer's Club)
- Prepare organisation to **meet new changes** through risk assessments, protocols and policies

Contact Us



- ❑ **Hotline** 2827 2827
- ❑ **Fax** 2877 7026
- ❑ **Website** www.pcpd.org.hk
- ❑ **E-mail** enquiry@pcpd.org.hk
- ❑ **Address** 12/F Sunlight Tower, 248 Queen's Road East, Wanchai