Safeguarding Privacy in eHRSS

Ms Jace CHIU
Senior Executive Officer (eHR) Special Duties
eHRSS Privacy Protection Office

“Data is the oil, some say the gold, of the 21st century”

- Joe Kaeser
CEO of Siemens

“The difference between oil and data is that the product of oil does not generate more oil, whereas the product of data will generate more.”

- Piero Scaruffi,
Cognitive scientist and author of “History of Silicon Valley”

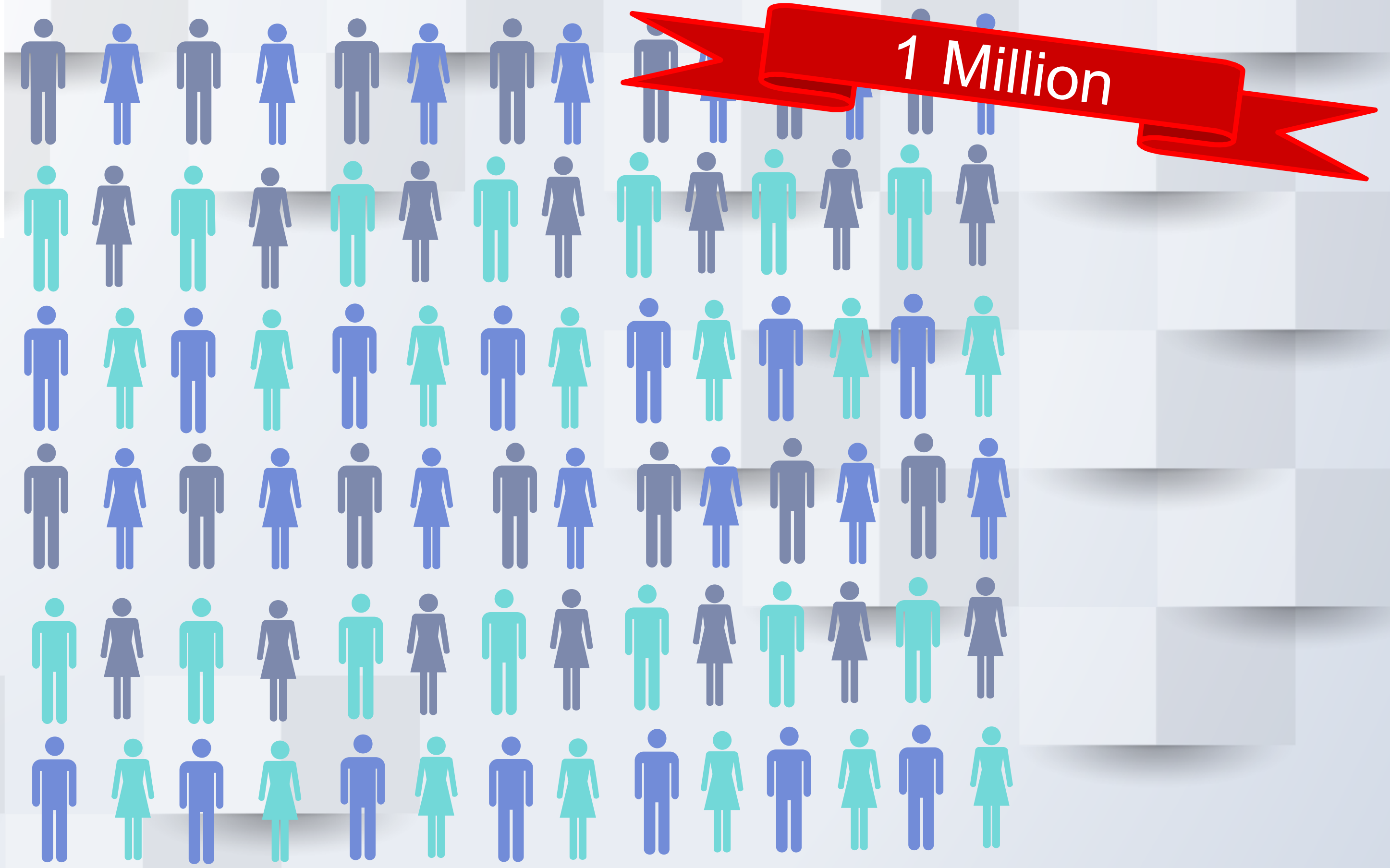
In 2018, someone’s identity was stolen every 3 seconds!

How much is your information worth?

Category	Price (USD)
Email Address & Password	$0.7-2.3
Credit Card	$8-22
Driver License	$20
Medical Record (each episode)	$1.5-10
Complete Medical Record	Up to $1000

Source: https://keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html

醫健通
ehealth
香港特別行政區政府 HKSAR GOVT



From Compliance to Accountability

- Responsibility to put in place adequate policies and measures to ensure and demonstrate compliance

- Translate legal requirements into risk-based, verifiable and enforceable corporate practices and controls

Security and Privacy
Ease of Use

Taking a proactive approach to data protection

List of privacy safeguards in eHRSS

- ❑ Patient controlled consent management
- ❑ Role-based access control for healthcare professionals
- ❑ Secure log in and full data protection
- ❑ 2-factor authentication
- ❑ Cyber-security protection
- ❑ Legal protection from PDPO and eHRSSO
- ❑ Various privacy protection related guidelines
- ❑ Privacy Protection Office

Privacy Protection Office

Key responsibilities of Privacy Protection Office (PPO)

❑ Establish and implement privacy-related controls for upholding the data protection principles;

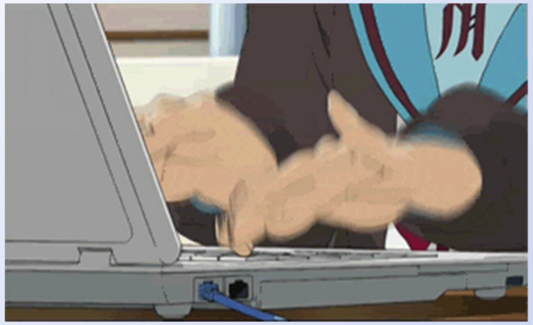
❑ Coordinate and conduct Privacy Impact Assessment(s) and Privacy Compliance Assessment(s);

❑ Perform audits on accesses to eHRSS including suspicious accesses in eHRSS;

❑ Conduct investigation on suspected data breach and privacy incidents;

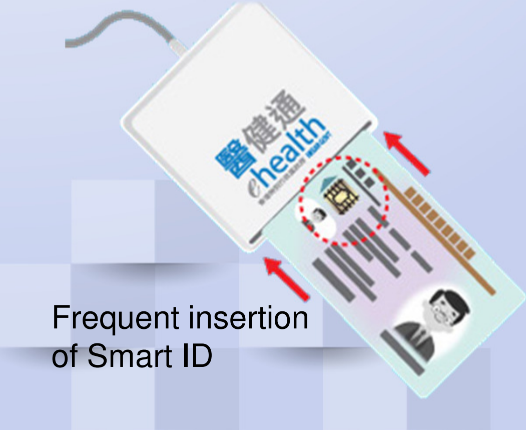
❑ Promote personal data protection in eHRSS

Suspicious accesses in eHRSS



Frequent trial on access key

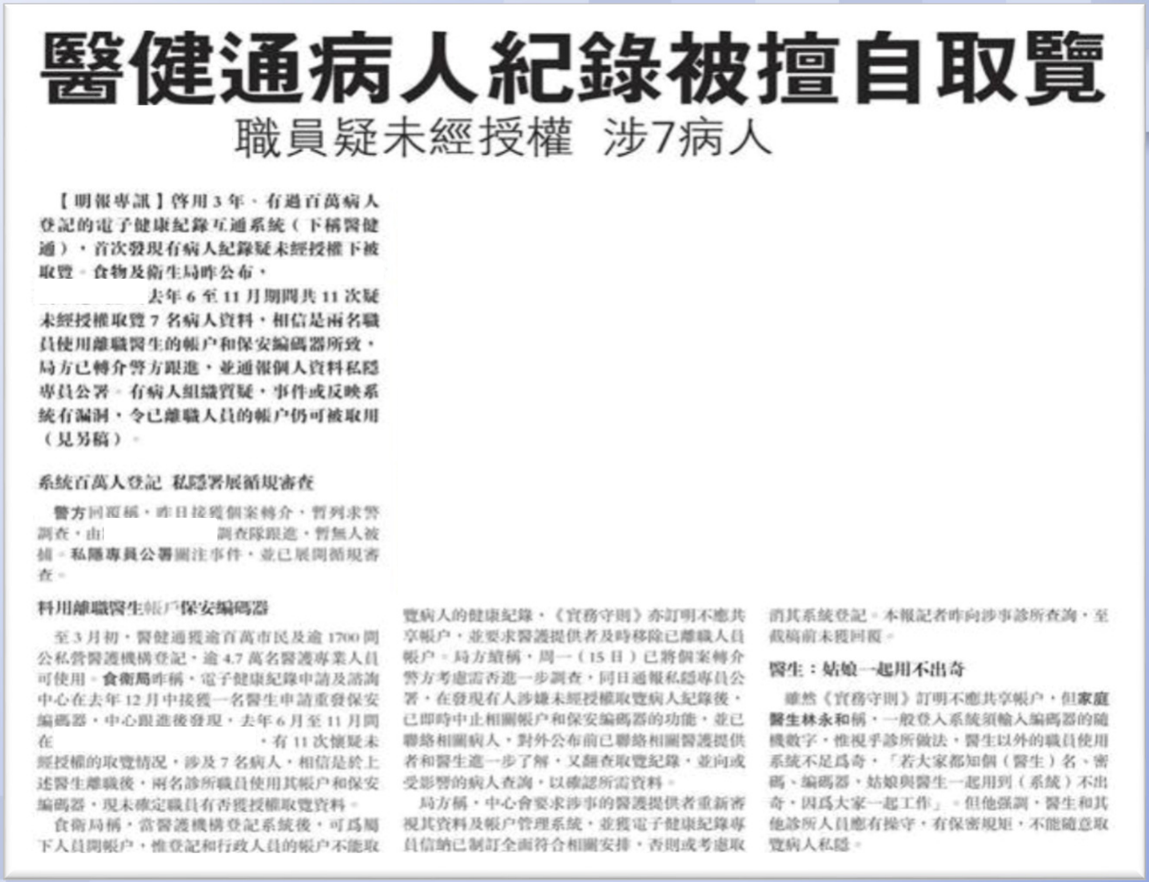
Frequent logon within a short period of time



Frequent insertion of Smart ID

Users (HCProfs/ User Admin) report on suspicious accesses

Patients report on suspicious accesses



醫健通病人紀錄被擅自取覽

職員疑未經授權 涉7病人

【明報專訊】啓用3年、有過百萬病人登記的電子健康紀錄互通系統（下稱醫健通），首次發現有病人紀錄疑未經授權下被取覽。食物及衛生局昨公布，去年6至11月期間共11次疑未經授權取覽7名病人資料，相信是兩名職員使用離職醫生的帳户和保安編碼器所致，局方已轉介警方跟進，並通報個人資料私隱專員公署。有病人組織質疑，事件或反映系統有漏洞，令已離職人員的帳户仍可被取用（見另稿）。

系統百萬人登記 私隱署展循規審查

警方回覆稱，昨日接獲個案轉介，暫列求警調查，由調查隊跟進，暫無人被捕。**私隱專員公署**關注事件，並已展開循規審查。

料用離職醫生帳户保安編碼器

至3月初，醫健通獲逾百萬市民及逾1700間公私營醫護機構登記，逾4.7萬名醫護專業人員可使用。**食衞局**昨稱，電子健康紀錄申請及諮詢中心在去年12月中接獲一名醫生申請重發保安編碼器，中心跟進後發現，去年6月至11月間在，有11次懷疑未經授權的取覽情況，涉及7名病人，相信是於上述醫生離職後，兩名診所職員使用其帳户和保安編碼器，現未確定職員有否獲授權取覽資料。

食衞局稱，當醫護機構登記系統後，可爲屬下人員開帳户，惟登記和行政人員的帳户不能取覽病人的健康紀錄，《實務守則》亦訂明不應共享帳户，並要求醫護提供者及時移除已離職人員帳户。局方續稱，周一（15日）已將個案轉介警方考慮需否進一步調查，同日通報私隱專員公署，在發現有人涉嫌未經授權取覽病人紀錄後，已即時中止相關帳户和保安編碼器的功能，並已聯絡相關病人，對外公布前已聯絡相關醫護提供者和醫生進一步了解，又翻查取覽紀錄，並向或受影響的病人查詢，以確認所需資料。

局方稱，中心會要求涉事的醫護提供者重新審視其資料及帳户管理系統，並獲電子健康紀錄專員信納已制訂全面符合相關安排，否則或考慮取消其系統登記。本報記者昨向涉事診所查詢，至截稿前未獲回覆。

醫生：姑娘一起用不出奇

雖然《實務守則》訂明不應共享帳户，但**家庭醫生林永和**稱，一般登入系統須輸入編碼器的隨機數字，惟視乎診所做法，醫生以外的職員使用系統不足爲奇，「若大家都知個（醫生）名、密碼、編碼器，姑娘與醫生一起用到（系統）不出奇，因爲大家一起工作」。但他強調，醫生和其他診所人員應有操守，有保密規矩，不能隨意取覽病人私隱。

We need YOU in privacy protection

How?

1.

Use eHRSS appropriately

2.

Manage the eHRSS account properly

As a User

- □ Do not share account
- □ Use a strong password and Do not disclose it
- □ Keep your token safe
- □ Staying on top of your account
- □ Logout when you won’t use the system even just for a while
- □ When you leave your employer, please
    - □ Keep the token or return it to Registration Office yourself
    - □ Change your password before you leave

As a HCP

- □ Remind your staff not to share accounts
- □ Assign appropriate user roles
- □ Check eHRSS User Access Log regularly
- □ Review your list of active accounts regularly
- □ When an employer resigned and left your institution, you should
    - □ “End the relationship” or Terminate the account

3.

Handle patient’s, their SDM’s and AP’s personal information with care

As a **User**

You should handle

❑ the Hong Kong Identity Card

❑ the completed joining and sharing consent forms

with care

Chan xxx xxx
31-12-1972
15-01-1991
COPY

As a HCP

- You should comply with the eHRSS Data Retention Policy
  - Physical copies of program administrative forms *(including application forms for registration or update of information, giving or revoking consent, etc.)* and supporting documents *(including copy of identity document)* for HCR registration…shall be kept for 6 months after the date of completion of registration process

- You should dispose the records securely and safely

4.

Report to us any suspicious activity or suspected privacy incident in eHRSS

Hotline: 3467 6230

Email: ehr@ehealth.gov.hk

Privacy Kit of eHRSS

@ eHRSS Website: https://www.ehealth.gov.hk/

- Privacy Policy of eHRSS

- Safe Use of User Account Leaflet

Electronic Health Record Sharing System

KEEP YOUR USER ACCOUNT SAFE

Unauthorised Access to the Electronic Health Record Sharing System (eHRSS) is Unlawful and Strictly Prohibited

✓ Access eHRSS only with your own account

✗ Don't use others' accounts
Unauthorised access is liable to prosecution

Tips for eHRSS Account User

1. Don't disclose or share your user name, password and security token
2. Set a strong password and change it regularly
3. Keep your account login information and security token safe
4. Log out eHRSS after use
5. Report lost security token immediately
6. Report suspicious access immediately

Tips for User Administrator

1. Assign individual account for each user
2. Ensure only authorised healthcare professionals can access patients' electronic health records
3. Update user information timely
4. Close account for departed user timely
5. Record and manage access rights assigned to each authorised user
6. Report suspicious access immediately

醫健通 ehealth

Secure and Privacy Protected Access to Patients' Health Records

3467 6230 3467 6099 www.ehealth.gov.hk ehr@ehealth.gov.hk

- Roles and Responsibilities of User Administrator in eHRSS

- Personal Information Collection Statement (User Account Creation Request Form)

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

保障・尊重個人資料
Protect, Respect Personal Data

Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals)

The Electronic Health Record Sharing System Ordinance[1] came into operation on 2 December 2015. It provides a legal basis for the collection, sharing, use and safe keeping of patients' health data under the Electronic Health Record Sharing System ("**System**"). The System is an information infrastructure platform for healthcare providers (including doctors and other healthcare professionals) in both the public and private sectors to, with the consent of a patient, access and share the patient's health record in the System for healthcare-related purposes.

The System will commence operation in the first quarter of 2016. Healthcare providers may visit the website of the System (www.ehealth.gov.hk) for more details.

The Relationship between the Personal Data (Privacy) Ordinance and the System

Patients' health records in the System amount to personal data, which is protected under the Personal Data (Privacy) Ordinance[2]. Healthcare providers and the Commissioner for the Electronic Health Record, as the data users, should act in accordance with the requirements under the Electronic Health Record Sharing System Ordinance as well as the Personal Data (Privacy) Ordinance (including the Six Data Protection Principles) when handling patients' health records in the System.

The functions and powers of the Privacy Commissioner for Personal Data, Hong Kong under the Personal Data (Privacy) Ordinance in relation to personal data in the System include:

➤ handling complaints of suspected breaches of the Personal Data (Privacy) Ordinance[3] and initiating investigation if necessary;

[1] Chapter 625 of the Laws of Hong Kong
[2] Chapter 486 of the Laws of Hong Kong
[3] Please refer to the Complaint Handling Policy issued by the Office of the Privacy Commissioner for Personal Data, Hong Kong ("PCPD")

Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals) / February 2016 1

- Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals)

Electronic Health Record Sharing System
and Your Personal Data Privacy
[10 Privacy Protection Tips]

PCPD.org.hk

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

- Electronic Health Record Sharing System and Your Personal Data Privacy (10 Privacy Protection Tips)

- FAQs for Healthcare Provider and Professional

用得小❤

用得安❤

THANKS!