About "Systematic Training Programme & Certification for Healthcare and IT Practitioners"

"Systematic Training Programme & Certification for Healthcare and IT Practitioners" ("STPC") is one of the latest training initiatives of eHealth Consortium, sponsored by the eHealth Record Office of Food and Health Bureau, under the scheme of "eHR Engagement Initiative (EEI)" in November 2010.

eHealth Consortium ("eHC"), the organizer of STPC, aims to infuse 700 members of eHealth stakeholders (Healthcare/IT Professionals, Practitioners and Executives) with essential eHealth understandings and hands-on skills. STPC consists of three courses:

1. "eHealth Awareness Course for eHealth Practitioners"
2. "eHealth Training for eHealth Executives"
3. "Proficiency Training for eHealth Professionals"

eHealth Consortium would like to thank all course facilitators and participants for their support in ehealth.

About the Organizer

Established since 2005, eHealth Consortium ("eHC") is one of the major non-profit making organizations in Hong Kong leading ehealth advocacy in the region and we are the prime agency bridging healthcare and IT industries to advance the development of eHealth in Hong Kong and Mainland China. Over the years, our efforts are focused on three key areas, namely data standardization, education and capacity building, and facilitating pilot projects for the advancement of eHealth applications. We work closely with the healthcare and the ICT sectors to offer training programs, conferences, and seminal events for ehealth stakeholders.

As of February 2011, eHC is an organization of 25 Corporate Members, 18 NGO Members and over 250 Individual Members from healthcare and IT.

For more information about eHC, please visit www.ehealth.org.hk.

Systematic Training Programme and Certification for Healthcare and IT Practitioners

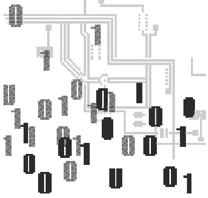
電子健康聯盟
eHealth Consortium Ltd

eHR and Data Privacy

March 2011

Ir Dr. K. P. Chow
Centre for Information Security & Cryptography
Department of Computer Science
The University of Hong Kong

What is eHR?



eHR – Electronic Health Record

- A systematic collection of electronic health information about individual patients or populations
- It is a record in digital format that is capable of sharing across different health care settings, by being embedded in network-connected enterprise-wide information systems
- It includes demographics, medical history, medication and allergies, …

eHR – Pros and Cons

Advantages	Disadvantages
Reduction in health care cost	Implementation cost
Improve quality of care	Implementation time
Promote evidence-based medicine	Privacy concerns
Record keeping and mobility	Legal issues

Privacy Concerns

- Health Insurance Portability and Accountability Act (HIPAA) (US 1996) establish rules for access, authentications, storage, auditing, and transmittal of electronic medical records
- European Union Directives to protect the processing and free movement of personal data, including eHR.
- Personal Information Protection and Electronic Document Act (PIPEDA) extension (Canada 2002) establish rules on the use, disclosure and collection of personal data include eHR.

Privacy Threat in U.S.

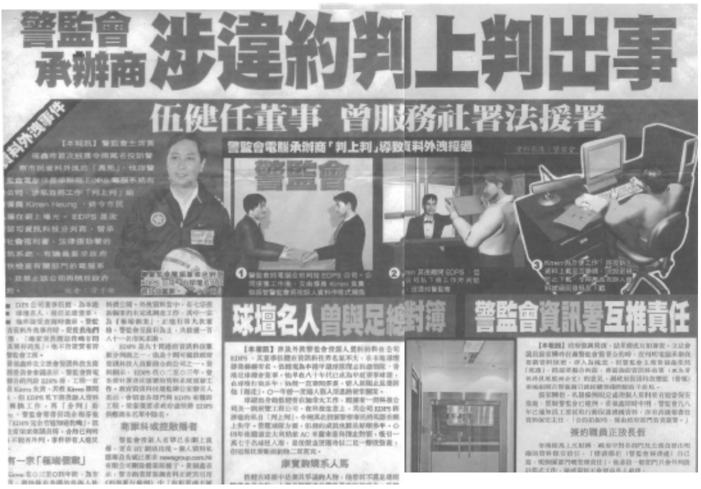
- According to Prof. J.M. Appel, the number of people needs to access to a truly interoperable national system was estimated to be 12 million in US
- While hospitals keep careful tabs on who accesses the charts of VIP patients, they are powerless to act against a *meddlesome pharmacist in Alaska who looks up the urine toxicology on his daughter's fiancé in Florida, to check if the fellow has a cocaine habit.*

How about Hong Kong?

Cases related to Leakage of Personal Data in Hong Kong

IPCC Case (Mar 2006)

- 20,000 complaint files against the Hong Kong Police available on the Internet



警監會承辦商 涉違約判上判出事

資料外洩事件

伍健任董事 曾服務社署法援署

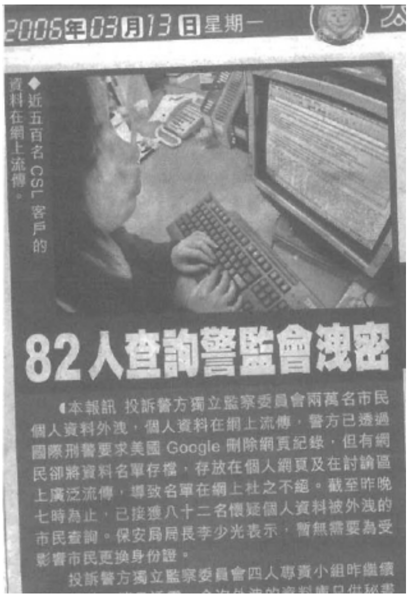
警監會電腦承辦商「判上判」導致資料外洩經過

[illegible]

球壇名人曾與足總對簿

警監會資訊署互推責任

[illegible]



2006年03月13日星期一

◆近五百名CSL客戶的資料在網上流傳。

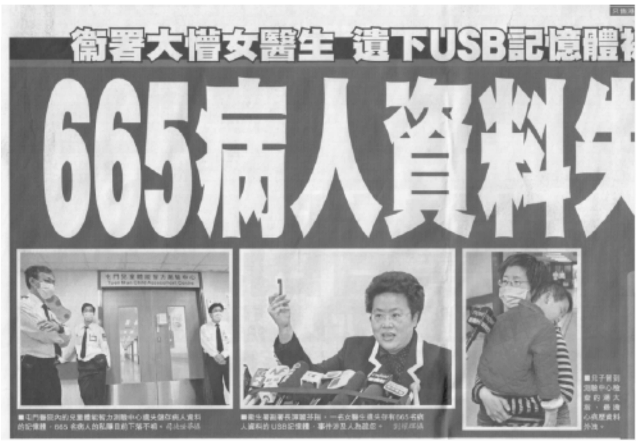
82人查詢警監會洩密

本報訊 投訴警方獨立監察委員會兩萬名市民個人資料外洩，個人資料在網上流傳，警方已透過國際刑警要求美國 Google 刪除網頁紀錄，但有網民卻將資料名單存檔，存放在個人網頁及在討論區上廣泛流傳，導致名單在網上杜之不絕。截至昨晚七時為止，已接獲八十二名懷疑個人資料被外洩的市民查詢。保安局局長李少光表示，暫無需要為受影響市民更換身份證。

投訴警方獨立監察委員會四人專責小組昨繼續

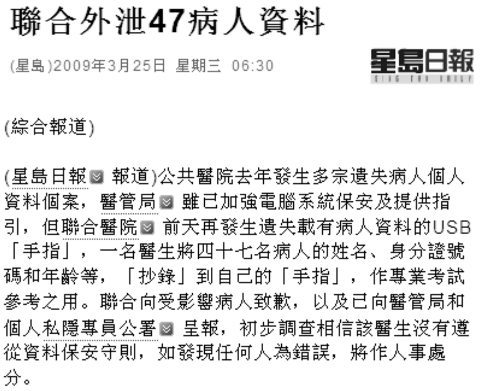
HOSPITAL AUTHORITY

- Numerous cases from Apr 2008 to Mar 2009 involving medical doctors lost USB drives with patients' personal data



衞署大懵女醫生 遺下USB記憶體袋

665病人資料失



聯合外泄47病人資料

(星島)2009年3月25日 星期三 06:30

星島日報

(綜合報道)

(星島日報 報道)公共醫院去年發生多宗遺失病人個人資料個案，醫管局 雖已加強電腦系統保安及提供指引，但聯合醫院 前天再發生遺失載有病人資料的USB「手指」，一名醫生將四十七名病人的姓名、身分證號碼和年齡等，「抄錄」到自己的「手指」，作專業考試參考之用。聯合向受影響病人致歉，以及已向醫管局和個人私隱專員公署 呈報，初步調查相信該醫生沒有遵從資料保安守則，如發現任何人為錯誤，將作人事處分。

Personal Data (Privacy) Ordinance and Data Protection Principles

Personal Data (Privacy) Ordinance – PDPO

- Enacted in 1995 and came into force on 20 Dec 1996
- Overseen by the Privacy Commissioner for Personal Data
- Regulates the use by individuals, companies, public bodies and government departments of data relating to living individuals who can reasonably be identified from the data

Data Protection Principles

- Key requirement of the PDPO is compliance with the 6 data protection principles
- A data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice is required or permitted under the Ordinance

Six data protection principles

- Principle 1- Purpose and manner of collection of personal data
- Principle 2 - Accuracy and duration of retention of personal data
- Principle 3 - Use of personal data
- Principle 4 - Security of Personal data
- Principle 5 - Information to be generally available
- Principle 6 - Access to personal data

Key terms

- Personal data: any data relating directly or indirectly to a living individual, from which it is practically for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable
- Data user: a person who controls the collection, holding, processing or use of the data
- Data subject: the individual who is the subject of the data
- The Code Book: Code of Professional Conduct, Medical Council of Hong Kong

PRINCIPLE 1 - PURPOSE AND MANNER OF COLLECTION OF PERSONAL DATA

- Purpose of collection
  - The data must only be collected for a lawful purpose directly related to a function or activity of the data user
  - the collection should be necessary for, or directly related to, that purpose
  - The data collection must be adequate but not excessive for that purpose
  - During data collection, the data collector must take all practicable steps to inform the relevant individual whether it is obligatory to supply the data and, if so, the consequence of failing to do so

PRINCIPLE 1 - PURPOSE AND MANNER OF COLLECTION OF PERSONAL DATA

- Manner of collection
  - Personal data must only be collected through means which are lawful and fair and in the circumstances of the case
  - Unlawful collection: intercepts mail without authority
  - Unfair collection: fails to disclose the identity of the data collector

Does eHR contain personal data?

- YES
- Are you collecting personal data?
  - Usually YES, such as
- Did you specify the purpose of collection?
- Did you collect the personal data in proper manner?
  - Usually YES, how?

Principle 2 – Accuracy and duration of retention of personal data

- All personal data should be accurate, up to date and kept no longer than necessary
- Inaccuracy: incorrect, misleading, incomplete, obsolete
- An organization should have a retention policy, and computer systems should be audited whether the retention policy is enforced

IMPLEMENTATION PROBLEMS

- How often should we update the patient’s personal data?
- How long should we retain the patient’s personal and medical data?

According to the Code Book, all doctors have the responsibility to maintain systematic, true, adequate, clear and contemporaneous medical records.

PRINCIPLE 3 – USE OF PERSONAL DATA

- Personal data may not be used for the purpose it is collected or a directly related purpose unless the express consent of the data subject is obtained
- Use includes transfer or disclosure

SOMETHING TO KEEP IN MIND

- Did you transfer the patient's personal data to another doctor (data collector)?
- Did your patient know that such transfer exist?
  - Implied consent: most patients understand their health information needs to be shared within the healthcare team

According to the Medical Council of Hong Kong's Code of Professional Conduct, it is the responsibility of any doctor who is intending to cease practising medicine to ensure that patient's medical records are appropriately handled and transferred.

DISCLOSURE

- When disclosing information, it should be annoymised if possible, and include only the minimum information for the purpose
- Without consent:
  - May be obliged to disclose information to comply with the law or prevent serious harm
  - Must carefully consider the arguments for an against the disclosure and be able to justify your reason

PRINCIPLE 4 – SECURITY OF PERSONAL DATA

- Personal data held by a data user should be protected against unauthorized or accidental access, processing, erasure or other use
- Following factors should be considered:
  - the kind of data and the harm that could result if any of those things should occur;
  - the physical location where the data are stored;
  - any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;
  - any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
  - any measures taken for ensuring the secure transmission of the data.

PRINCIPLE 5 – INFORMATION TO BE GENERALLY AVAILABLE

- All practicable steps shall be taken to ensure that a person can
  - ascertain a data user's policies and practices in relation to personal data;
  - be informed of the kind of personal data held by a data user;
  - be informed of the main purposes for which personal data held by a data user are or are to be used.

Principle 6 – Access to personal data

- A data subject shall be entitled to
  - (a) ascertain whether a data user holds personal data of which he is the data subject;
  - (b) request access to personal data-
    - i. within a reasonable time;
    - ii. at a fee, if any, that is not excessive;
    - iii. in a reasonable manner and
    - iv. in a form that is intelligible
  - (c) be given reasons if a request referred to in (b) is refused;
  - (d) object to a refusal referred to in (c);
  - (e) request the correction of personal data;
  - (f) be given reasons if a request referred to in (e) is refused, and
  - (g) object to a refusal referred to in (f).

Hong Kong Medical Association Patient's Rights and Responsibilities

- Right of information
  - A patient should have a reasonable and balanced understanding of the sickness he is suffering from, know what treatment you will receive, and related information
- Right of confidentiality
  - The personal information of patients should be highly confidential

CAN YOU AMEND YOUR MEDICAL RECORD?

- HIPAA (US) gives everyone the right to see, copy, and request to amend their own medical records
- How about in Hong Kong?
  - PDPO gives you the right to modify your own personal data

PERSONAL CONFIDENTIAL DATA

- Personal data: e.g. HKID card no.
- Confidential data: e.g. an individual's medical history
- Personal confidential data: linking the personal data with his/her confidential data
- The PDPO is about personal data only

Problem: eHR data privacy, confidential and security

Key Concepts

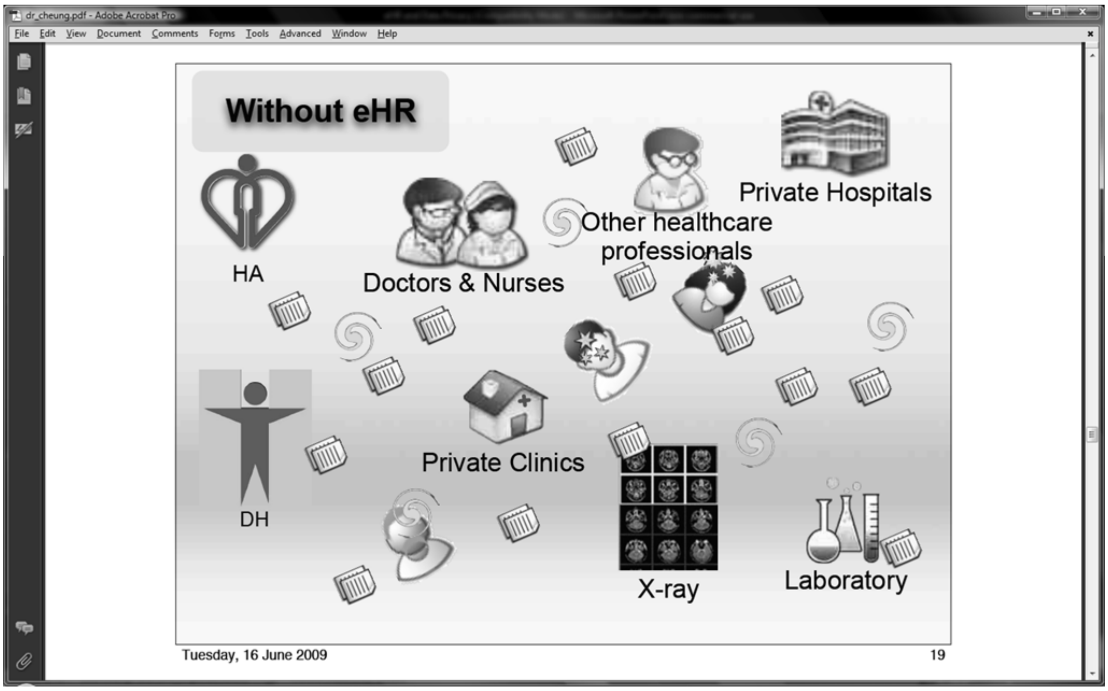
- Privacy is the right to control who has access to one's own data, what they can do with those data, and under what circumstances
- Confidentiality is the protection of data from inappropriate or unauthorized access or use
- Security is the physical protection and preservation of data

Small Clinic

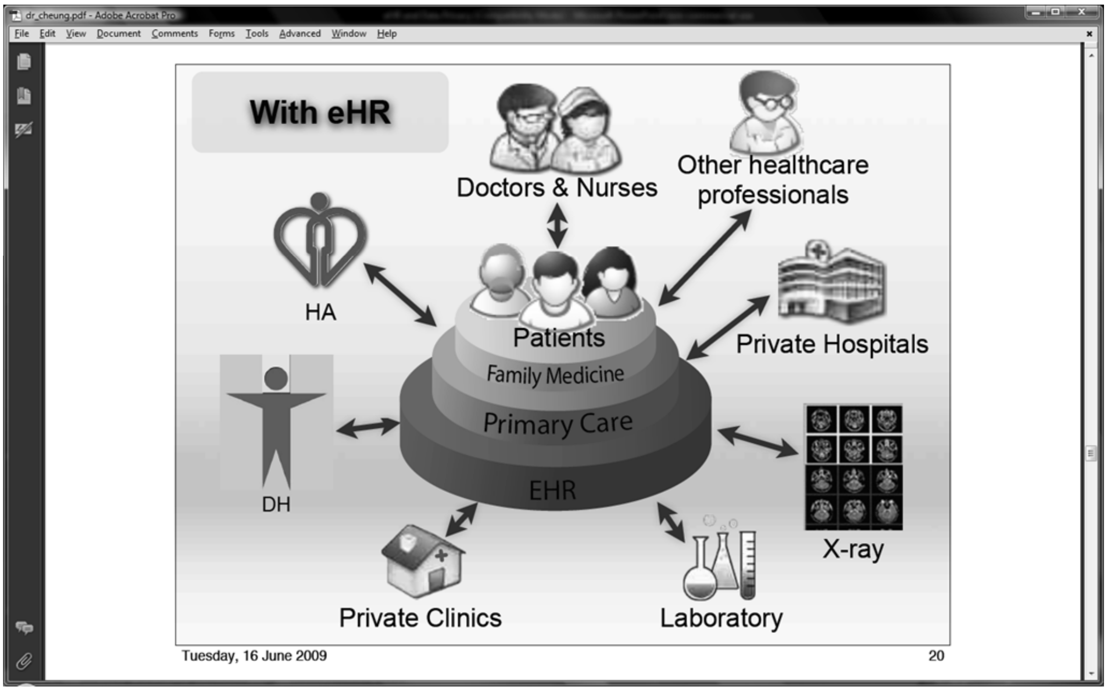
- Paper or digital records
- Security:
  - Small number of trusted personnel
  - Physical security
- Privacy:
  - Purposes of collection
  - Accuracy and retention of data
  - Transfer of data
  - Data security
  - Access to data

HK-Wide Electronic Health Record (eHR)

UNORGANIZED (DR. CHEUNG 2009)



Coordinated and Structured (Dr. Cheung 2009)


dr_cheung.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help

With eHR

Doctors & Nurses

Other healthcare professionals

HA

Patients

Family Medicine

Primary Care

EHR

Private Hospitals

DH

X-ray

Private Clinics

Laboratory

Tuesday, 16 June 2009

20

What is in eHR?

- Personal particular for identification and contact, e.g. name, HKID, DoB (personal data)
- Health data, e.g. weight, height, blood type
- Medical data, e.g. diagnosis, lab test results, radiological images

How will the eHR be protected?

- Legal framework
  - Protected by the Personal Data (Privacy) Ordinance (PDPO)
  - eHR office will formulate a legal framework to safeguard the privacy and security of eHR sharing system and its daa
- Assessment studies will be performed:
  - Privacy Impact Assessment
  - Privacy Compliance Audit
  - Security Risk Assessment and Security Audit

Purposes of Assessments

- Study
  - Who can access the data?
  - Who has the right to control the access of data?
  - How a person and/or the health provider can be identified and authenticated?
  - How data can be protected from unauthorized access?
  - How data integrity is maintained in the systems?

Basic computer security principles (CIA):
•Confidentiality
•Integrity
•Availability, Authenticity, Accountability

SOME KEY CHARACTERISTICS OF FUTURE EHR

- Sharing of data
  - On the enterprise network
  - May transfer data through Internet
  - Through portable storage media, e.g. USB drive
- Accountability
  - Who has access the data?
  - What has modified the data?
- Security
  - Is the network under attack?
  - Do the machines infected by virus?

DATA LEAKAGE INCIDENTS IN THE PAST

- Two major sources:
  - The Internet
  - The USB thumb drives

WHY THERE ARE SO MANY SECURITY AND PRIVACY PROBLEMS ON THE INTERNET?

- Inherits from the original Internet - the "ARPAnet":
  - Link up academic institutions and research organizations
  - No design consideration for security and privacy
- Grows from research network into a network used by general public
  - Still based on the original infrastructure: TCP/IP
  - "New" services supported: search engine and archives, newsgroup, P2P
  - Malware: virus, worm, spyware, rootkit

Do Internet users aware of the problems?

THE USB THUMB DRIVE PROBLEM

- Too convenience
- Data access without control
- Users "un-awareness"

IT Security and Personal Data Protection

IT Security Framework

- Access control
- Cryptography

IT Security Framework – Access control

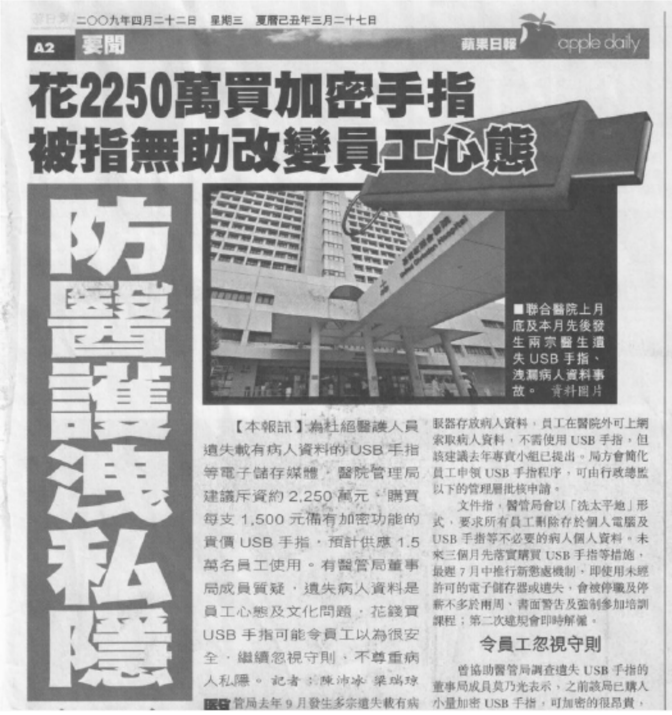
- Availability: prevention of unauthorized withholding of information or resources
- Authenticity: able to verify the origin of data
- Accountability: audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party

IT Security Framework - Cryptography

- Confidentiality: prevention of unauthorized disclosure of information
- Integrity: prevention of unauthorized modification of information
- Non-repudiation: when data or messages are exchanged over a network, neither the sender can deny sending it nor the receiver can deny receiving it

WILL ACCESS CONTROL/ENCRYPTION SOLVE THE PROBLEM?

- Access control
- Cryptography
  - Expensive USB drive with hardware encryption



二〇〇九年四月二十二日　星期三　夏曆己丑年三月二十七日

A2 要聞　蘋果日報 apple daily

花2250萬買加密手指 被指無助改變員工心態

防醫護洩私隱

■聯合醫院上月底及本月先後發生兩宗醫生遺失USB手指、洩漏病人資料事故。　資料圖片

【本報訊】為杜絕醫護人員遺失載有病人資料的USB手指等電子儲存媒體，醫院管理局建議斥資約2,250萬元，購買每支1,500元備有加密功能的貴價USB手指，預計供應1.5萬名員工使用。有醫管局董事局成員質疑，遺失病人資料是員工心態及文化問題，花錢買USB手指可能令員工以為很安全，繼續忽視守則，不尊重病人私隱。記者：陳沛冰 梁瑞琼

醫管局去年9月發生多宗遺失載有病

服器存放病人資料，員工在醫院外可上網索取病人資料，不需使用USB手指，但該建議去年專責小組已提出。局方會簡化員工申領USB手指程序，可由行政總監以下的管理層批核申請。

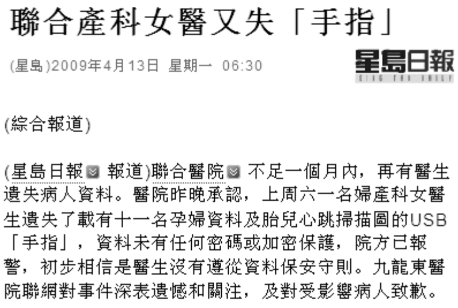
文件指，醫管局會以「洗太平地」形式，要求所有員工刪除存於個人電腦及USB手指等不必要的病人個人資料。未來三個月先落實購買USB手指等措施，最遲7月中推行新懲處機制，即使用未經許可的電子儲存器或遺失，會被停職及停薪不多於兩周、書面警告及強制參加培訓課程；第二次違規會即時解僱。

令員工忽視守則

曾協助醫管局調查遺失USB手指的董事局成員莫乃光表示，之前該局已購入小量加密USB手指，可加密的很昂貴，

HOSPITAL AUTHORITY CASE (APR 2009)

- Medical doctor lost her USB drive which contained patients' personal data

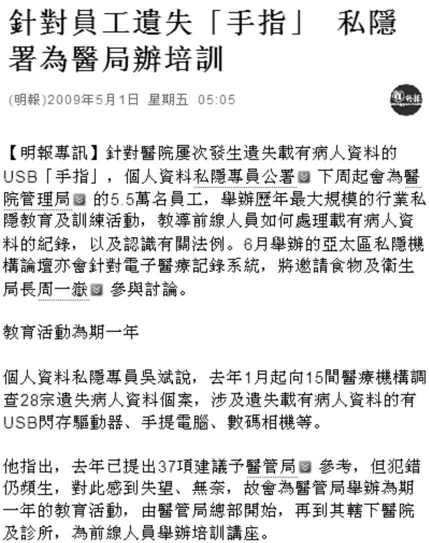


聯合產科女醫又失「手指」

(星島)2009年4月13日 星期一 06:30　星島日報

(綜合報道)

(星島日報☒ 報道)聯合醫院☒ 不足一個月內，再有醫生遺失病人資料。醫院昨晚承認，上周六一名婦產科女醫生遺失了載有十一名孕婦資料及胎兒心跳掃描圖的USB「手指」，資料未有任何密碼或加密保護，院方已報警，初步相信是醫生沒有遵從資料保安守則。九龍東醫院聯網對事件深表遺憾和關注，及對受影響病人致歉。



針對員工遺失「手指」　私隱署為醫局辦培訓

(明報)2009年5月1日 星期五 05:05

【明報專訊】針對醫院屢次發生遺失載有病人資料的USB「手指」，個人資料私隱專員公署☒ 下周起會為醫院管理局☒ 的5.5萬名員工，舉辦歷年最大規模的行業私隱教育及訓練活動，教導前線人員如何處理載有病人資料的紀錄，以及認識有關法例。6月舉辦的亞太區私隱機構論壇亦會針對電子醫療記錄系統，將邀請食物及衛生局長周一嶽☒ 參與討論。

教育活動為期一年

個人資料私隱專員吳斌說，去年1月起向15間醫療機構調查28宗遺失病人資料個案，涉及遺失載有病人資料的有USB閃存驅動器、手提電腦、數碼相機等。

他指出，去年已提出37項建議予醫管局☒ 參考，但犯錯仍頻生，對此感到失望、無奈，故會為醫管局舉辦為期一年的教育活動，由醫管局總部開始，再到其轄下醫院及診所，為前線人員舉辦培訓講座。

WHAT'S WRONG?

Gap between IT security and data protection principles

Personal Data (Privacy) Ordinance in Hong Kong

Data protection principles

Principles	IT Security Framework
Principle 1 – Purpose and manner of collection of personal data	×
Principle 2 – Accuracy and duration of retention of personal data	×
Principle 3 – Use of personal data	×
Principle 4 – Security of personal data	√
Principle 5 – Information to be generally available	×
Principle 6 – Access to personal data	×

WHICH PROBLEM DO THEY SOLVE?

- The IT security framework solve the security problem only
- It only solves “their” problem, but not the “right” problem
  - Typical software engineering issue

TECHNOLOGIES AND DATA PROTECTION PRINCIPLES

Should be handled by different technologies:

Principles	Technologies
Principle 1 – Purpose and manner of collection of personal data	**New technologies and framework required** (purpose and binding)
Principle 2 – Accuracy and duration of retention of personal data	
Principle 3 – Use of personal data	
Principle 4 – Security of personal data	**IT security** (security and accountability)
Principle 5 – Information to be generally available	**User interface technology** (user rights and data accuracy)
Principle 6 – Access to personal data	

THE GAP

- Current access control technology:
  - Can someone access the file owned by *Mr. X*?
  - Implemented in most operating systems, e.g. MS Windows, Linux, ….
- Outstanding issue:
  - Can someone execute the *program* owned by data controller *access* the data belongs to *Mr. X* *today*?
  - Can someone *make a copy* of the data belongs to *Mr. X* collected by the *data controller* on *12 June 2009*?

Some suggestions for eHR implementation

RECOMMENDED PROCEDURES FOR YOUR IT SUPPORT STAFF

- Should not have access to personal data unless formally approved
- Should be instructed not to access nor copy any personal data from system

RECOMMENDED PROCEDURES FOR YOUR DATA HANDLING STAFF

- Should be informed if they are going to input personal data
- Should be instructed not to access nor copy any personal data from the system
- Access personal data in database should be documented
- Should exercise proper controls and diligence at all stages of the operations including
  - Startup, access of database
  - Export data from database
  - Copy or backup of database

Recommended procedures with external IT contractor

- Data user should not release information that contains personal data to its IT contractor
- Data user should clearly inform its IT contractor whenever the IT contractor is going to carry out any task that involves the handling of personal data
- Information that passed from the data user to its IT contractor that contains personal data should contain proper label.
- Data user should ensure that the IT contractor carries out appropriate checks on their staff
- Data user should keep track and proper records of all the personal data that has been given to its IT contractor
- Data user should give clear instructions to the IT contractor in respect of the use, transmission, storage and destruction of the personal data given to it

Recommended procedures on accessing personal data in DB

- All access to personal data in the database should be authorized, monitored and accounted for.
- All database copy/backup from database that contains personal data should be authorized, monitored and accounted for.
- All database exported from database that contains personal data should be authorized, monitored and accounted for.
- Reports on the above database operations should be produced and reviewed regularly.

Recommended procedures for exporting data

- Export of personal data should be authorized.
- Exported personal data on removable storage media, e.g. floppy diskettes, CDs, USB drives, should be properly labeled.
- Computer printed copy that contain personal data should contain proper label.
- Email that contains personal data should have the content encrypted and properly labeled.

Recommended procedures for personal data destruction

- The retention period of personal data in IT systems should follow the relevant legal and regulatory requirements, and the industry standards.
- Whenever the personal data is no longer used, it should be destroyed properly.
- For personal data within a PC/server, the PC/server's hard disk should be sanitized.
- All backup copies and exported copies should be destroyed.
- All printed copies should be destroyed.
- Proper records should be kept of the destructions.

電子健康聯盟
eHealth Consortium Ltd

Thank you

Systematic Training Programme and Certification for Healthcare and IT Practitioners

電子健康聯盟
eHealth Consortium Ltd

COMMON THREATS AND SOLUTIONS IN DAILY OPERATION OF PERSONAL DATA

Lawrence Tam
Exco Member, iProA
CEO, LogicToken Co. Ltd.

AGENDA FOR THE DAY

- Paper Records vs eHR
  - Principal Threats and Defenses
  - Technical Challenges
  - Software Issues
- Preventive Measures, Planning and Execution
  - Audit Trail within eHealth Systems
  - Access Control: Single vs Multi-factor Authentication
  - The Four-Stage Recommendation

Paper Records

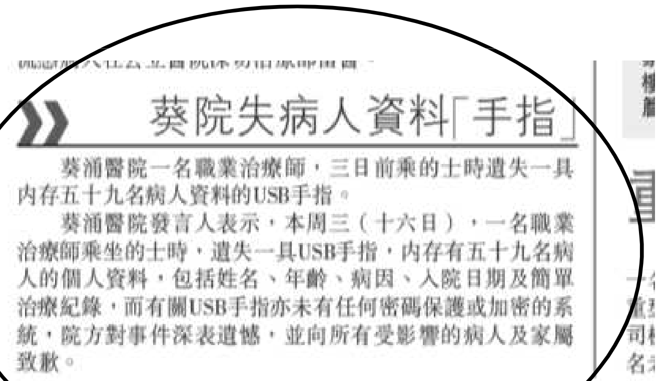
- *The Good:*
  - *Have been around for 100 years*
  - *Proven, mature and simple filing system usually by patients' names but labor intensive*
  - *Retrieval and collation can be nightmare but great privacy and protection for the patients*
- *The Bad:*
  - *Paper records are horrible as far as legibility is concerned*
  - *Rarely sharing among multi medical practitioners for the same patient, leading to delay of diagnosis and treatments that may save one's life*
- *The Ugly:*
  - *In case of accidental loss, almost impossible to recover (i.e. fire or water damages, etc.)*

Electronic Records

- *Yesterday*
  - *Transition to e-Records in the 80's through retyping or scanning to image, yet the process was tedious*
  - *Retrieval / collation have improved but still challenging*
- *Today*
  - *Separate eHR systems among private and public practitioners, leading to health records being available in fragmented / isolated manners*
  - *Still mostly back office capturing after patient's visit and then printing for paper filing, i.e. Legibility has improved*
- *Tomorrow*
  - *Ideally eHR moves the patient information capturing to the front end of the process, having the doctors to capture the details while s/he is performing diagnosis*
  - *Having a centralized database at least on regional basis to improve efficiency, reduce costs, and boost the quality of health care*

Nobody wants to see this happen!

- Numerous incidents of leaking patient's information through electronic devices due to non-encrypted records on non-protected USB thumb drive and other means.



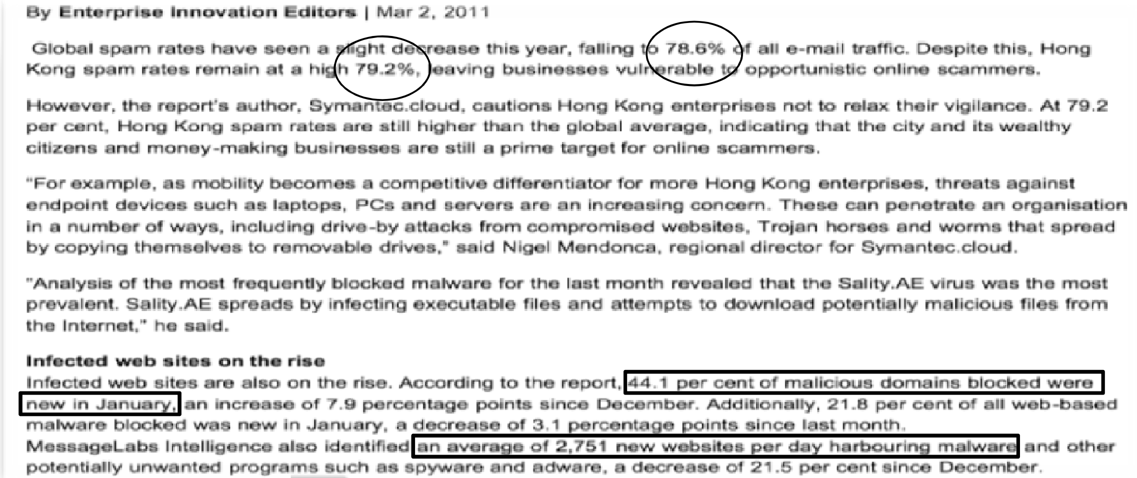
葵院失病人資料「手指」

葵涌醫院一名職業治療師，三日前乘的士時遺失一具內存五十九名病人資料的USB手指。

葵涌醫院發言人表示，本周三（十六日），一名職業治療師乘坐的士時，遺失一具USB手指，內存有五十九名病人的個人資料，包括姓名、年齡、病因、入院日期及簡單治療紀錄，而有關USB手指亦未有任何密碼保護或加密的系統，院方對事件深表遺憾，並向所有受影響的病人及家屬致歉。

February, 2011

Hong Kong is Hacker's Resort



By Enterprise Innovation Editors | Mar 2, 2011

Global spam rates have seen a slight decrease this year, falling to 78.6% of all e-mail traffic. Despite this, Hong Kong spam rates remain at a high 79.2%, leaving businesses vulnerable to opportunistic online scammers.

However, the report's author, Symantec.cloud, cautions Hong Kong enterprises not to relax their vigilance. At 79.2 per cent, Hong Kong spam rates are still higher than the global average, indicating that the city and its wealthy citizens and money-making businesses are still a prime target for online scammers.

"For example, as mobility becomes a competitive differentiator for more Hong Kong enterprises, threats against endpoint devices such as laptops, PCs and servers are an increasing concern. These can penetrate an organisation in a number of ways, including drive-by attacks from compromised websites, Trojan horses and worms that spread by copying themselves to removable drives," said Nigel Mendonca, regional director for Symantec.cloud.

"Analysis of the most frequently blocked malware for the last month revealed that the Sality.AE virus was the most prevalent. Sality.AE spreads by infecting executable files and attempts to download potentially malicious files from the Internet," he said.

Infected web sites on the rise

Infected web sites are also on the rise. According to the report, 44.1 per cent of malicious domains blocked were new in January, an increase of 7.9 percentage points since December. Additionally, 21.8 per cent of all web-based malware blocked was new in January, a decrease of 3.1 percentage points since last month.
MessageLabs Intelligence also identified an average of 2,751 new websites per day harbouring malware and other potentially unwanted programs such as spyware and adware, a decrease of 21.5 per cent since December.

HK still top spammer target, despite global spam plunge

Hong Kong spam rates remain at a high 79.2%, leaving businesses vulnerable to opportunistic online spam

Concerns over Electronic Records

- *Identity theft and fraud*
- *Medical records being used / exposed without consent or misused for marketing*
- *Health care employees' access to personal data*
- *Risk of propagating incorrect information*
- *Careless exposure of personal data*
- *Accidental data corruption or loss*
- *Hardware failure / virus attack*

The Reality

- *It is not just a technical concern as technology can only do so much*
- *If our behavior on handling sensitive data does not improve, the best technology will not help*
- *Attention to personal data protection is everyone's responsibility along the chain…*
- *It is no different from handling paper documents*
- *Awareness of data privacy & security is an on-going exercise*
- *It is more a cultural issue!*

USER GROUPS

- *Patient and her/his family*
- *Medical practitioners (doctors, nurses, specialists, admin staff)*
- *Insurance companies*
- *Drug manufacturers*
- *Medical research centers*
- *Clinics / Hospitals*
- *Internal and contracted IT service providers (Hardware, Software, Network, etc.)*

MISSION OF IT SECURITY

- *Confidentiality – Privacy*
- *Authenticity – Only authorized access*
- *Integrity – No unauthorized tempering*
- *Protection – Limit on download / printing*
- *Non-repudiation – No denial of action / operation taken*

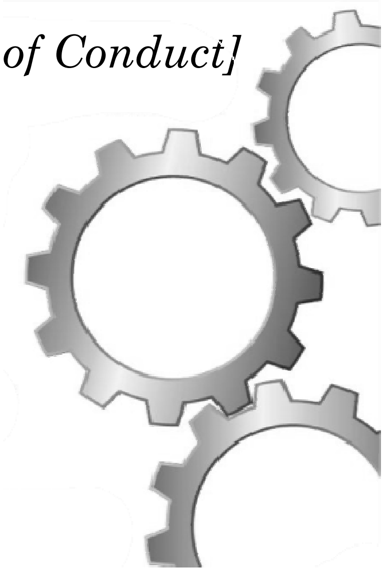
Things Can Be Addressed Technically

- *Network Encryption*
  - *Ensure no hacking / interception of data during transmission / remote access*
- *Data / File Encryption*
  - *S/W or H/W protection, particularly for portable devices such as USB thumb drive*
- *Application / Database Encryption*
  - *Ensure data confidentiality and integrity*
- *Authentication*
  - *Ensure accessibility only by authorized individuals*

Soft Issues and Challenges

- *Corporate and Public Culture*
- *Company policy, procedure and behavior*
- *Training and Reinforcement*
- *Observance of Access Policy*
- *PC and Storage Disposal Policy (no different from shredding paper documents)*
- *Compliance and Enforcement of Law and Regulation*
- *Management and staff commitment to IT security*
- *Dealing with employees committing data breaches and revenges by terminated / poorly appraised staff*

Security Management



- *Employment Policy & Practice [Code of Conduct]*
- *Data Handling Guideline*
- *Risk Assessment*
- *Corporate Governance*
- *Role-based vs Need-based Control*
- *Access in Open Area*
- *How much to disclose*
- *Data classification*
- *Surveillance*
- *Legal Regulation & Legislation*

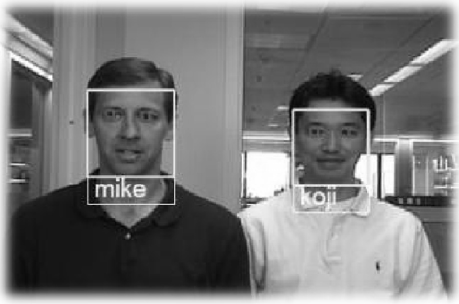
Security Audit

- *Audit Trail*
- *Change Control*
- *Content Monitoring*
- *Intrusion Detection and Prevention*
- *Fraud Discovery and Reporting*
- *Access Log Management*
- *Logical Access of Database*
- *Physical Access and Storage of Sensitive Data*
- *Hierarchical vs Duty Based Segregation*
- *Access Control of Application*

Use of Audit Trail

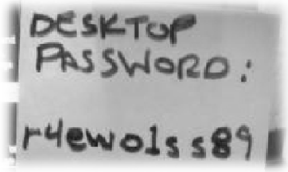
- Monitoring User Compliance to
  - Identify suspect or actual privacy breaches
  - Deter unauthorized access or "browsing"
- Quality Improvement
  - Role management
  - Access Management
  - Audit logging and reporting
- Forensic Investigation of
  - Privacy and security breaches and other incidents

Access Control



- *ID + Password*
- *E-Certificate / PKI*
- *OTP + Password*
- *Devices:*
  - *Biometric: Fingerprint/Iris/Face/Voice/Palm*
  - *Smart Card*
  - *Dongle*
  - *Mobile Device*

PASSWORDS



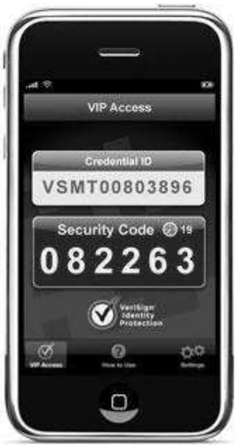
DESKTOP PASSWORD:

r4ewols s89

- *Too Simple*
  - *Birthday (990312)*
  - *Simple Words (health)*
  - *Revise of ID (password->drowssap)*
  - *Highest rate of usage are admin, 1234, abcd*
  - *Name of family member, close friend and pet (honey)*
- *The other extreme - Too Complicated / One Pass for ALL*
- *Suggestions:*
  - *Combination of upper and lower cases, number and even symbol (PW+np@0815)*
  - *At least 8-character long*
  - *Change regularly (at least every 3 months)*
  - *Never use common computers for emails, e-banking, etc.*
  - *Use OPEN wi-fi network with care*

MULTI-FACTOR AUTHENTICATION

- eCert / PKI – Public Key Infrastructure
- OTP – One Time Password
- Pictorial Key



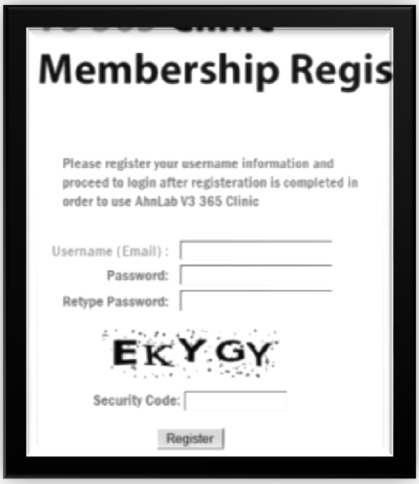
VIP Access

Credential ID

VSMT00803896

Security Code 19

082263



Membership Regis

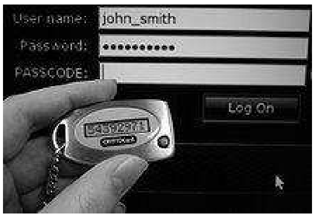
Please register your username information and proceed to login after registeration is completed in order to use AhnLab V3 365 Clinic

Username (Email) :

Password:

Retype Password:

Security Code:



User name: john_smith

Password: ●●●●●●●●●●

PASSCODE:

MALPRACTICES IDENTIFIED BY PCPD(NOTE 1)

- *Excessive collection of personal data*
- *Unfair Personal information collection statement (small print / lots of pages)*
- *Misuse of personal data for product/service promotion and cross-marketing*
- *"Bundled" Consent*

Note 1: PCPD - Privacy Commissioner for Personal Data

LEGISLATION AND REGULATIONS

- *"Octopus" episode has potentially exposed 2 million personal data to the world (what if these are hospital records)*
- *Roles & Responsibilities of Department of Privacy Commissioner for Personal Data (PCPD)*
- *More promotion, education and training regarding Privacy Awareness*
- *More stringent laws and regulations to deal with exposing and/or misusing individuals' personal information*

PRIVACY - BASIC HUMAN RIGHTS!

- *Four-Stage Suggestions for any Project / Process:*
- *Planning Stage:*
  - *Inclusion of personal data protection as an integral part of the corporate culture*
- *Before implementation:*
  - *Identify privacy related issues to minimize risk of privacy exposure (i.e. fingerprint access system: is it privacy intrusive?)*
- *During implementation:*
  - *Conduct regular audit to ensure compliance by all concerned parties and accordingly fine tune the process*
- *After implementation:*
  - *Enforce privacy policy and immediately report any breaches and threats to the authority*

Systematic Training Programme and Certification for Healthcare and IT Practitioners

電 子 健 康 聯 盟
eHealth Consortium Ltd

Q & A

For more information, please contact:

Lawrence Tam

Lawrence.Tam@LogicToken.com

+852 3748-9583