Protecting Personal Data Privacy & Security

NTEC

Tiki Hon

Updated 20130621

2. HA Data Access Principles

Dear colleagues, please be reminded of all these:

Data Access Principles

1. Purpose of Access
   - Patient under care
   - Organizational need-to-know
2. Keep the account to yourself, do NOT share account
3. ONLY access to information that is sufficient to carry out your duty
4. Keep the accessed data confidential
5. Access the data in a secured environment
6. Log off after use
7. All access are logged and subjected to audit
8. Breach of confidentiality is subject to disciplinary action/would be reported to the Police

Privacy Committee, NTEC Nov 2007

親愛的同事, 請注意下列守則:

資料數據使用守則

1. 使用的目的
   - 病人正接受治療護理
   - 有關機構需得悉相關的資料
2. 電腦帳戶爲個人擁有，故切勿共用
3. 只可提取履行工作所需的資料
4. 要把所得的資料數據保密
5. 在保密的情況下提取資料數據
6. 使用後請立即登出電腦帳戶
7. 每次使用均被記錄及受到審查
8. 違反保密條例者會遭受紀律處分或交予警方辦理

Privacy Committee, NTEC
Nov 2007

3. What is Sensitive Personal Data ?

1) Sensitive personal data must be protected

- **HKID (most sensitive) especially when in combination of:**

  such as any other clinical data (e.g. case summary) or personal data (e.g. phone, address, Date of Birth)

- **Full name +**

  any other clinical data (e.g. case summary)

  or personal data (e.g. phone, address, Date of Birth)

- What's New
- Mission and Vision

Structure
- Organization Chart
- People (Staff/CallList/Roster)
- Resource (Facility/Location/Equip)

Process
- Plan
- Policy/Protocol/Guideline
- Program
- new NTEC CQI
- Service
- Form

Outcome
- Report
- Audit
- Indicator
- Work & Resource

Sharing and Learning
- Education

Search

Search

(For Dept User Only)
- Calendar
- Meeting
- Minutes
- T&D
- Statistics
- e-Discussion
- Social Area (iPhoto/Event)
- Secured Shared Folder

IT Data Storage Devices Alerts & Form

(Link to: NTEC Information Technology Web)

Description

1 **Highlights** of Personal Data Security / 個人資料保安

2 **Enhanced Measures on Enforcing Personal Data** (NTEC/CCI/P-001-V1)
- Check list and action plan for all NTEC staff / departments w.e.f. fully by 15 June 2008
Cover memo, Standard Operation Procedure (SOP) (NTEC/CCI/P-001-V1) &
Checklist and action plan in PowerPoint

3. **NTEC Periodic Reminders on IT Security**

4 **Useful tools:**

(i) Adding password & encryption for:
- Acrobat Pro (Userguide / Online Demo)
- Ms-Word 2010(Userguide / Online Demo)
- Ms-Excel 2010(Userguide / Online Demo)
- MS-Powerpoint 2010(Userguide/ Online Demo)
- Outlook 2010(Userguide)
- MS-Word 2003 (Userguide / Online Demo)
- MS-Excel 2003(Userguide / Online Demo)
- MS-Powerpoint 2003(Userguide/ Online Demo)

(ii) Password & encryption for 7-Zip software
- Manual Installation 7-Zip Procedures (Userguide P.4 / Online Demo)
- Encrypt files/folders to a zip (Userguide P.5-7 / Online Demo)
- Add files to an existing encrypted zip file (Userguide P.8-10 / Online Demo)
- Modify and update content from an existing encrypted zip file (Userguide P.11 / Online Demo)
- Delete File from an existing encrypted zip file (Userguide P.13 / Online Demo)

(iii) NTEC PC & Accessories Inventory Management System

5 **Application Form for:**
(i) "**pink label**" for NTEC-procured removable storage device and mobile computing equipment [NTECITD-26] (Workflow)
(ii) "**white label**" for approved non-HA device that are used in work-related storage of confidential or sensitive data. [NTECITD-27] (Workflow)
(iii) **HOIT secure USB** Flash Drive from HOIT [NTECITD-28]
(Note: Please read carefully the Information Technology Circular (1/2008) from HAHO, "Enhanced measure on Enforcing Personal Data Security" - part 6 (Use of USB Flash Drives for Operational Purposes) before the application is made).

6 **HOIT Policies & Guidelines relating IT Data Storage Devices Alerts:**
- A Practical Guide to IT Security
- Clinical Data Policy Manual / Training material- Access to Clinical Data (click here for details)
- Electronic Communication Policy Jan/2005 (Circular / Information web)
- HAHO Information Security & Tips for Information Security Web
- HAHO Secure USB Flash Disk User Guide
- HAHO Security Alert Centre
- HOIT Circular 1/2009: HA's Policy on Information Security and Privacy
HOIT Circular 2/2008: Desktop Security Guidelines for Protecting and Preventing the Loss of Confidential Data in HA PCs, Notebooks and Personal Data Assistants (PDAs)

Online Demo For setting password and encryption for data files with personal data

Online Demo for Word 2010

http://ntec.home/fileEncryption/wordencryption.wmv

Mandatory Training

PERSONAL DATA SECURITY

(Chinese version / IT Data Storage Index Page

1. **All data files with identifiable personal data (IPD) (i.e. containing HKID no. and/or Full Name)** whether exported or manually created on PCs, removable storage devices and other mobile computing devices **must be encrypted and password protected.**

2. **If there is an operational need to share file with IPD, place the file in departmental secure web-based share folder.**

3. **If there is an operational need to download file with IPD onto USB flash drive, only use secure USB issued by HOIT.**

Final warning to all staff:
Violation of the Data Security policy will be subjected to disciplinary action.

For further information and how to encrypt / password protect file, please visit
http://nteciis02:3388/iHosp/ntec_itd/Public/Process/Guideline_Protocol/MobileStorageAlert/MobileStorageAlert.htm

Refer to *HAHO Information Technology Circular 1/2008* – *Enhanced measures on enforcing Personal data Security*
Updated on 24 Aug 2009

b. e-mail

Practice Guide

- If is justifiable under the two principles:
  - Patient-under-care
  - Organization need-to-know

- Do NOT send emails containing confidential personal data to external parties unless it is in accordance with HA or hospital policy

- For sending the email with patient data, whether intranet or internet, e.g.
  - Remove confidential personal data from the email
  - Or Encrypt files containing confidential personal data

Reference

- Personal Data Privacy Ordinance - Data Protection Principle 4
- Electronic Communication Policy

c. Facsimile

Practice Guide

- Any record which contains confidential personal data should be faxed with a Confidential Fax Cover
- Re-check correctness of recipient fax number

Reference

- Personal
- Manual of
  Chapter 5
  - http://i
    nt

Tips:
- Use re-dial function
- Use the function key (store the fax number in the machine)

e. Examples of Security of Personal Data

1a. Delivery of medical record, X-Ray film & specimen

運送醫療紀錄、X光片及血液樣本

Don't expose patient's data on medical record, x- ray film & specimen cover and leave those trolley unattended

不要 讓醫療紀錄、X光片及血液樣本封面及有病人資料位置外露，或隨便擺放沒有覆蓋醫療紀錄運送車

e. Examples of Security of Personal Data

1b. Delivery of medical record, X-Ray film & specimen

運送醫療紀錄、 X光片及血液樣本

Do Wear uniform & staff ID

Use document bags, trolley cover and trolley w/door

要 穿著制服及佩戴職員証

將醫療紀錄、 X光片及血液樣本放置於文件袋、有車簾或車門之手推車中

e. Examples of Security of Personal Data

2b. Unauthorized Access

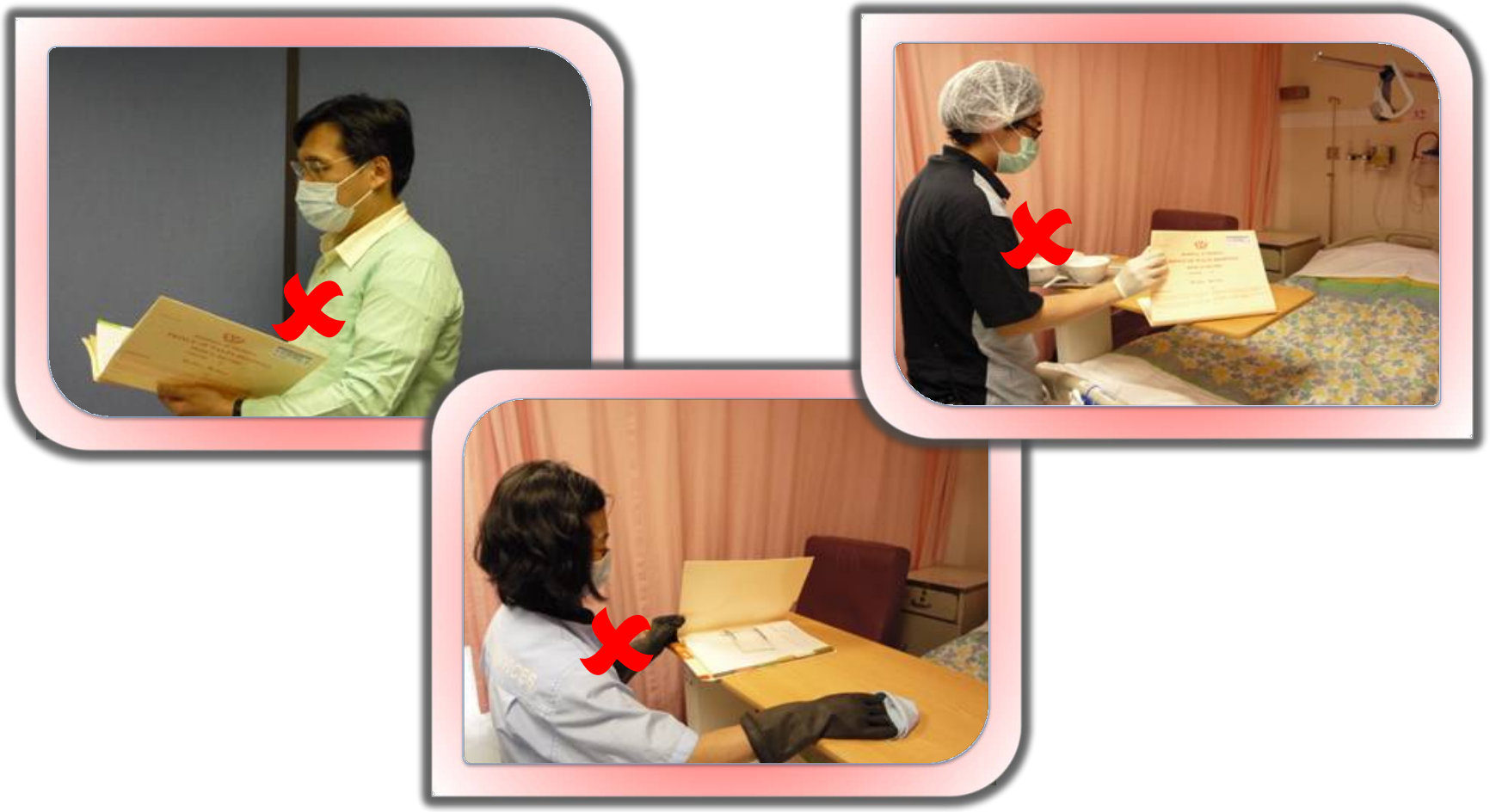
未經授權使用

Don't

Read medical records without authorization

不要

在未經授權下，翻閱病人醫療紀錄



e. Examples of Security of Personal Data

3a. Patient transportation

病人運送

Don't Expose patient's data

不要 讓病人資料外露

e. Examples of Security of Personal Data

3b. Patient transportation

病人運送

Do

put medical records & x- ray film into document bag in a designated place

要

把一概有關病人資料的文件，如醫療紀錄、x光片、血液樣本 等，放於文件袋中及放置在適當位置

e. Examples of Security of Personal Data

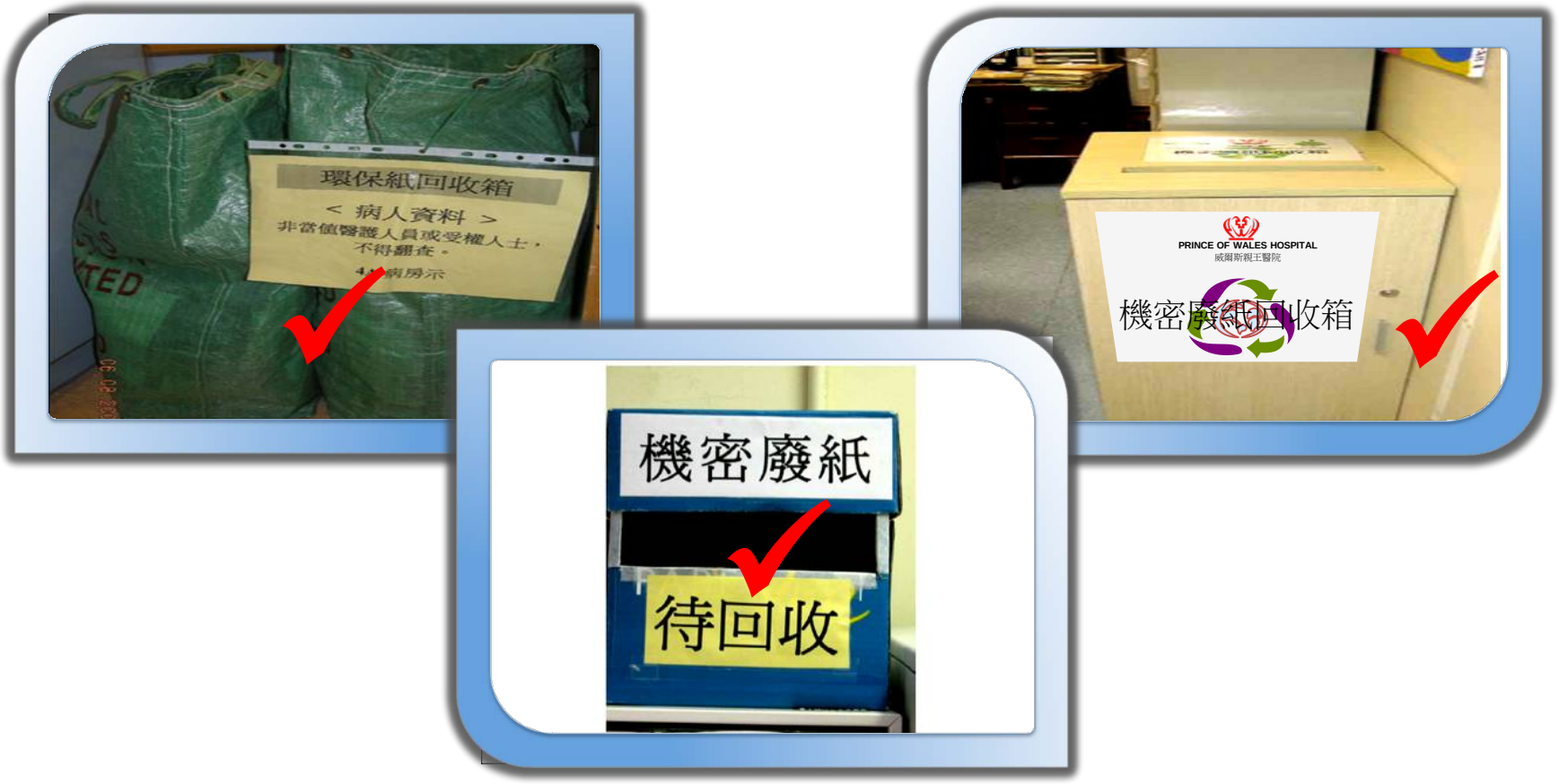
4b. Confidential Waste Paper Management
機密廢紙管理

Do

a. Dispose into specified container / bag only

要

甲. 將機密文件文件放於指定及有標籤的容器或袋中



e. Examples of Security of Personal Data

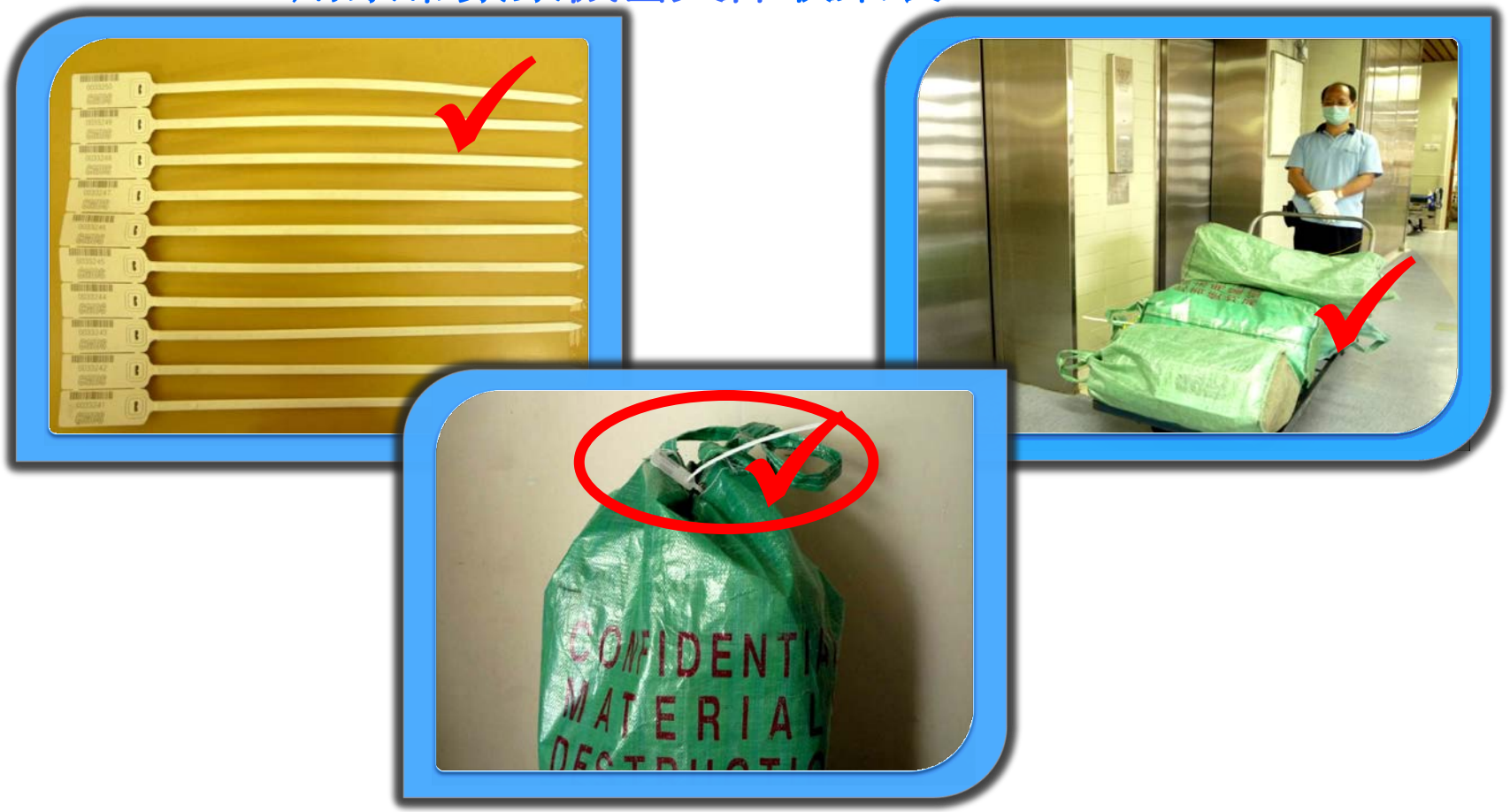
4c. Confidential Waste Paper Management
機密廢紙管理

Do

b. Secure confidential waste paper collection bag with sealing device

要

乙. 用索帶繫緊機密文件收集袋口



5. Reporting Incident of Loss of Personal Data

- Report to AIRS/Supervisor
- Report to the CISPO within 48 hours (from the date of report to AIRS) of the searching result
- Report to respective Hospital management
- Report to Security Office / Data Controller
- Report to Police if required

Useful Websites

- HA Information Security and Privacy

  http://infosec.home

http://infosec.home/Default.aspx?Lang=zh-TW

- NTEC Information Security and Privacy

  iHI&R@NTEC

http://nteciis02:3388/iHosp/ntec_hinr/Public/Process/Guideline_Protocol/data_security.htm

Questionnaire!

問卷

QUIZ for Personal Data Security and Privacy Training

	Question
1	When my staff carry their self-owned USB flash drive to work to store patient's personal data, should the USB flash drive be encrypted before downloading data?
2	Could I take original medical records and unencrypted file of patient personal data out of hospital without authorization from senior?
3	If I need to create some training materials with real patient clinical information, should the personal particulars (i.e. name, HKID no., date of birth, sex) be masked / deleted from the material?
4	A staff reports sick with haemorrhoid for 3 days. I need to send an e-mail to inform staff in the same team to arrange relieving staff. Should I inform them about his haemorrhoid condition as well?
5	I have taken some photos of newborns with a nursing colleague at the delivery room. Can I post these photos to my facebook to show my friends?
6	I am writing up a patient care plan after work at home. My son has just installed a P2P software like Foxy on the home computer. Is there any risk of leaking patient personal data to unauthorized people due to automatic uploading of file?
7	I have collected some completed HR forms from 4 wards. I have to send them to Cluster HR department by ward. I have put the return from wards into 4 envelops marking "Confidential" and clearly stated the location of the receiving HR department together with a serial number (i.e. 1 of 4, 2 of 4, 3 of 4 and 4 of 4). I have also prepared 3 sets of delivery notes, one for filing in our department, one for the signed return copy and the last one for filing in the receiving department. Are the above good practices when transporting confidential documents?
8	I have to send out a reply of a compliant case to PRO. Should I use HN, A&E or SOP No. instead of patient's name and HKID No.?
9	I shall leave HA and start my private practice next month. Should I retrieve a list of my patients and notify them to visit my private clinic in future?
10	My mother is admitted to the ward where I am working. But I am not involved in the patient care of her. Can I access her laboratory result under the "patient-under-care" principle?
11	I am assigned by hospital management to handle a patient complaint case on the treatment/care he received during hospitalization. Can I access to the electronic record of the patients for details under the "Organizational Need-to-know" principle?
12	I wish to request for a laboratory test on blood cholesterol for myself. Can I do that in CMS (Clinical Management System) by myself?
13	I'm planning the staff roster for next month, one of the colleague is on sick leave. Can I access the concerned colleague's CMS / ePR to facilitate my planning?

	Answer
1	Yes. Should be encrypted by EERM (Endpoint Encryption for removable Media) program.
2	No. All medical records should be securely kept in hospital premises and patient personal data should be encrypted.
3	Yes. Patient personal data should not be displayed during training.
4	No. The medical condition is personal data of the staff.
5	No. Staff shall not take pictures without consent. The pictures of newborn should not be disclosed without consent.
6	Yes. Should only do office work on computer without installation of P2P software like Foxy.
7	Yes.
8	Yes. The file should be further encrypted with password. Password has to be sent to the receiver separately.
9	No. This violates the use of data access principle.
10	No. The patient-under-care principle is not applicable in this case.
11	Yes.
12	No. This violates the data access principles
13	No. This violates the data access principles

Thank You !

多謝

Hospital Data Controller

NTEC CISPO	Ms Tiki Hon	26322418 (pager) 7382 1693
AHNH	Ms Carrie Wong	26893530
BBH	Mr Jimmy Tsui	26458899
NDH	Ms. Willie Sung	26837041
PWH	Mr Ng Ho Kai	26322075 (pager) 7382 2327
SCH	Ms Esther Law	26367240
SH	Ms Canice Cheiu	26367746
TPH	Ms Carrie Wong	26893530