Data Security

1. The Hospital Authority owns all clinical data that are created or collected in the course of patient care at HA institutions.

2. Access to the patient data is governed by the principles of patient under care and organizational need-to-know basis.

3. All staff are responsible for the safety & confidentiality of the patient data and to prevent unauthorized use.

4. The person who performs the data export in any means which involves the duplication of individually identifiable patient data, such as data download, printing or transcription is responsible for the usage and protection of the exported data which must comply with the PD(P)O principles and A Draft Paper on Release of Patient's Information.

5. Download of identifiable patient data to any mobile storage device such as notebook, USB, PDA, external hard-drive must be prohibited unless approval is granted by HCE.

6. Appropriate measures must be taken to protect the security of the exported data e.g. using encryption and password, keeping the exported data safely in a secured area.

7. All the unused and expired identifiable patient data should be deleted.

8. Identifiable patient data must not be transferred via internet e-mail.

9. For any loss of patient data, the staff must report to the department head immediately. The department head should consider to report the case to the Police as appropriate.

10. Breach of confidentiality and security is subject to disciplinary action.

11. Useful Link

- Mobile Storage Alert (http://ntec.home/ntecitd/MobileStorageAlert.htm)
- Frequently Asked Questions - Clinical Data Policy (http://informatics.home/mediawiki/index.php/Clinical_Data_Policy_-_Frequently_Asked_Questions)
- A Practical Guide to IT Security (http://ha.home/infosec/document/A_Practical_Guide_to_IT_Security_EN.doc)
- Clinical Data Policy Manual (http://informatics.home/mediawiki/index.php/Clinical_Data_Policy_Manual)
- Electronic Communications Policy Jan 2005 (http://ha.home/ho/ecp/ecp-intro.htm)

資料保安

1. 醫院管理局擁有由轄下機構提供病人治療護理期間所建立或收集之臨床資料。

2. 查閱病人資料須依從病人正接受治療護理及有關機構需得悉相關的資料的守則。

3. 所有職員均有責任保護病人資料，以保密其資料，並防止未經授權的人士閱讀或使用。

4. 所有人士進行任何方法輸出包含有可識別的病人資料，例如資料下載、印製或抄寫，必須有責任遵從《個人資料(私隱)條例》、《發放病人資料草稿》及保護其輸出的資料。

5. 除非獲得醫院行政總監授權同意，否則嚴禁下載存有可識別的病人資料至任何流動電子儲存媒體，如手提電腦、USB記憶體、電子手帳、外置硬碟等。

6. 必須採取適當的保安措施以保護輸出資料，例如使用加密程序及密碼保護，存放輸出資料於保安的地方。

7. 刪除所有未經使用及已滿期限之可識別的病人資料。

8. 不得透過互聯網電子郵件傳送可識別的病人資料。

9. 如有任何病人資料遺失，職員必須立即向部門主管匯報，部門主管須考慮將事件交予警方辦理。

10. 違反保密及保安條例者會遭受紀律處分。

常用結連

- Mobile Storage Alert (http://ntec.home/ntecitd/MobileStorageAlert.htm)
- Frequently Asked Questions - Clinical Data Policy (http://informatics.home/mediawiki/index.php/Clinical_Data_Policy_-_Frequently_Asked_Questions)
- A Practical Guide to IT Security (http://ha.home/infosec/document/A_Practical_Guide_to_IT_Security_EN.doc)
- Clinical Data Policy Manual (http://informatics.home/mediawiki/index.php/Clinical_Data_Policy_Manual)
- Electronic Communications Policy Jan 2005 (http://ha.home/ho/ecp/ecp-intro.htm)