Tips for Information Security

GUARDING THE INFORMATION

(Mainly extracted from "A PRACTICAL GUIDE TO IT SECURITY FOR EVERYONE WORKING IN HOSPITAL AUTHORITY from HOIT, revised on May 2008")

DO:

- Be discreet with confidential data at all times.
- **Ensure the PCs, notebooks, USB flash drives, RAM cards or mobile computing devices should support access control and/or password "lockdown" functions.**
- Encrypt the confidential data created by yourself.
- Keep passwords private and change them periodically.
- Erase confidential data immediately when no longer in use.
- Erase data before disposing or repairing PC, notebook, mobile computing device and removable storage device.
- Blank the computer screen before the next patient comes into a consulting or treatment room.
- Report to your management if loss of confidential data has happened.
- Telephone the recipient to ensure he/she is present to collect a fax when you send one containing patient identifiable information.
- Dispose of confidential print-outs properly.

Tips for Information Security

GUARDING THE INFORMATION

(Mainly extracted from "A PRACTICAL GUIDE TO IT SECURITY FOR EVERYONE WORKING IN HOSPITAL AUTHORITY from HOIT, revised on May 2008")

DON'T:

- **Disclose any patient or other personal information to anyone without authority.**
- **Download or use any unauthorized or unknown software such as peer-to-peer applications (e.g. Foxy) in your PC or notebook which work-related documents stored and/or when connecting to HA network locally or remotely.**
- **Download, copy or backup confidential data into PCs, notebooks, USB flash drives, RAM cards or mobile computing devices such as PDA or smartphone. If it is authorized to do so, only the minimum essential confidential data should be used and the confidential data must be encrypted.**
- **Leave your computer logged on when your computer/terminal is unattended**
- **Leave removable storage devices, discs, tapes, print-outs, fax messages lying around.**