Security Tips for Health Care Voucher Scheme and Using the eHealth System (Subsidies)

(Enrolled Health Care Providers)

1. **Physical Security**
    (a) All computer components should be physically secured and be placed in a safe area.
    (b) The equipments are well equipped to protect against physical or natural disasters.
    (c) Remove and erase all storage media before disposal of computers.
    (d) Documents related to voucher account creation and voucher claims should be physically stored in a safe area, such as locked filing cabinets or properly locked office areas.
    (e) Documents related to voucher account creation and voucher claims should be accessed only by authorized personnel.
    (f) Proper and full records related to voucher account creation should be retained in the concerned places of practice. They should be retained for a period of not less than 7 years after the date of the Voucher Account Creation Form.
    (g) Proper and full records related to voucher claims should be retained in the concerned places of practice. They should be retained for a period of not less than 7 years after the date of the Consent of Voucher Recipient to Use Vouchers.

2. **Backup & Recovery**
    (a) Perform data backup in the eHealth System (Subsidies), as considered necessary, regularly.
    (b) Backup copies should be kept in a secure place and accessible only on a need-to-know basis.

3. **Combat Computer Virus**
    (a) Install on-line anti-virus software to continuously real-time check and automatically clean for computer viruses and malicious codes, for any files, emails, or data going through the firewall or individual information servers.
    (b) Virus signature and malicious code definition should be updated regularly. The update should be configured as automatic and update frequency should be at least on daily basis.
    (c) If automatic update of anti-virus software is not possible (e.g. mobile computers which are often not attached to networks), update should be done manually at least once a week.

(d) Users should also note that from time to time, there could be ad-hoc or serious virus outbreaks. If so, users should immediately update with the latest virus signature and malicious code definition in order to protect against virus outbreak.

(e) Regularly perform computer virus and malicious code scanning for the host machine where the information servers are installed.

4. Access Control Security

(a) Computer should be accessed by authorised users only.

(b) Password-prompted computer screen locks should be set up.

5. Password Management

(a) Passwords should be regularly changed.

(b) Refer to “Password Do’s and Don’ts” at Annex.

6. Use of Removable Media for Computers and IT Systems

(a) Removable media include but not limited to flash memory devices, USB drives portable hard disks, CD, DVD, RAM disks, floppy disks, tapes and cartridges.

(b) Portable electronic devices containing classified information should be kept under continuous supervision when in use, and stored in physically protected areas appropriate for that classification when not in use.

(c) Enrolled Health Care Provider (EHCP) and his Data Entry staffs should not store identifiable personal data in removable storage media

(d) Identifiable personal information should not be transferred outside the EHCP’s places of practice by any means, including but not limited to portable electronic devices, electronic mails and messages.

7. Use of HCVS Authentication Token

(a) Authentication token should be physically secured and be placed in a secure area.

(b) Authentication token should be well stored for prevention from physical or natural disasters.

(c) Authentication token should be accessed and handled by authorised personnel only.

(d) EHCPs should report the loss of tokens to the Department of Health. The Department will de-activate the lost tokens and issue replacement tokens, after the respective fee has been paid.

Annex

Password Do’s and Don’ts

DOs

1. Do use a password with a mix of at least six mixed-case alphabetic characters, numerals and special characters.
2. Do use different passwords for different systems with respect to their different security requirements and value of information assets to be protected.
3. Do use a password that is difficult to guess but easy for you to remember, so you do not have to write it down.
4. Do use a password that you can type quickly, without having to look at the keyboard, so that passers-by cannot see what you are typing.

DON’Ts

1. Do not use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
2. Do not use your first, middle or last name in any form.
3. Do not use your spouse's or child's name.
4. Do not use other information easily obtained about you. This includes ID card numbers, license plate numbers, telephone numbers, birth dates, the name of the street you live on, etc.
5. Do not use a password with the same letter like “aaaaaa”.
6. Do not use consecutive letters or numbers like "abcdefgh" or "23456789".
7. Do not use adjacent keys on the keyboard like "qwertyui".
8. Do not use a word that can be found in an English or foreign language dictionary.
9. Do not use a word in reverse that can be found in an English or foreign language dictionary.
10. Do not use a well-known abbreviation. This includes abbreviation of Government department name, project name and district, etc.
11. Do not use a simple variation of anything described in 1-10 above. Simple variations include appending or prepending digits or symbols, or substituting characters, like 3 for E, $ for S, and 0 for O.

12. Do not use a password with fewer than six characters.
13. Do not reuse recently used passwords.