Colorectal Cancer Screening Programme (Programme)
Security Tips for Enrolled Health Care Providers

(a) Documents related to the Programme should be (i) kept in safe custody and handled vigilantly; (ii) physically stored in a safe area, such as locked filing cabinets or properly locked office areas; (iii) accessed only by authorised personnel; and (iv) retained in the concerned place of practice (i.e. enrolled Health Care Institution).

(b) All computer components should be physically secured and be placed in a safe area.

(c) Computer system and software should be updated with latest security patches applied. Licensed / legal computer software should be used and use of peer-to-peer software (e.g. Foxy or Bit Torrent…etc.) should be avoided. Appropriate anti-virus and anti-spyware should be installed.

(d) Computer should be accessed by authorised users only. Password-prompted computer screen locks should be set up.

(e) Passwords should be regularly changed.

(f) Authentication token should be placed in a secure area, well stored, and be accessed and handled by authorised personnel only. Loss of tokens should be reported to the Electronic Health Record Registration Office as soon as possible.

(g) When authorised staff log into the CRC-IT System of the electronic Health Record Sharing System (eHRSS), any records containing the clinical or personal information shown on the computer screen should not be seen by unrelated third parties (e.g. consider the direction of the screen and/or use privacy filters).

ENDS