ELECTRONIC SIGNATURE

Policy

The electronic signature process will create a magnetic impulse that will be considered the legal equivalent to the handwritten signature or initials.

The BC Cancer Agency accepts the electronic signature process for authentication of patient records by the medical staff. This process is to be used when deemed appropriate by BCCA.

Site Directives: VCC
IV-60 Documentation By Trainees

Description
The electronic signature process at BCCA will require the authentication of the signer's identity (authorized physician) by use of a confidential password system. This electronic signature will be adopted or authorized by the physician to be the legally binding equivalent of the physician's signature.

The password system will consist of the password for access to the Cancer Agency Information System (CAIS) applied to the signature process. The password will be encrypted when stored. Passwords will not be sent over the networks unless encrypted.

The requirements for the electronic signature process are:

1. Application of the CAIS password in conjunction with the signature process. The CAIS password contains the following criteria:
   - Password duration: maximum (42 days) and minimum 1 day.
   - Reuse of passwords: no reuse of previous eight passwords.
   - Password length (minimum 7 characters).
   - Log-on attempts: user will be locked out after 5 failed log-on attempts within 45 minutes. The count will be reset every 45 minutes.
   - Encryption of CAIS password when stored or sent over networks.

2. Signature of a password confidentiality agreement indicating the physician is the only one who has access to and will use the CAIS password code. (Appendix 1)

3. Application of the electronic signature will be preceded by the opportunity to :
   - Review entries for completeness and accuracy.
   - Correct or modify entries as needed.

4. Deletion or alteration of the electronic document will not be permitted within the system once the electronic signature has been applied. Addenda to entries will provide a means to add information if errors are identified after a signature has been applied. All addenda documents will require physician signature.

   For documents where a signature is not required, the information system will not permit deletion or alteration to any document after 14 days from date of creation (refer to Policy IV-C-50).

5. The system technology will support the following signature document standards:
   - accurate date and time stamps for:
     a) event time
     b) document creation time
     c) signature time
     d) document access time
     e) document modification (amendment time)
   - organization source
   - patient identifier
   - document identifier

6. All transcribed BCCA signature reports shall display in clear text the printed name (surname and initial) and the date and time the signature was completed.

   Non transcribed documents stored electronically shall electronically display name (surname and initial), date and time the electronic signature process was completed.

7. It shall be possible for multiple parties to sign a document if required in record completion policies.

8. Countersignatures (refer to IV-60): For procedures requiring countersignatures, identification of the order of the application of the signatures will be available for procedures requiring countersignatures.

9. Electronic signatures shall be verifiably bound to their respective

electronic records to ensure the signatures cannot be excised, copied or otherwise transferred to falsify another record.

10. Security: Security and user authentication are essential components of the electronic signature process. Security is the protection of a system and the data within the system from unauthorized access or modification. Security will be addressed by:

    - Use of confidential password system.
    - Signature of an Electronic Signature and Password Confidentiality Agreement (Appendix I). This signed statement by the physician indicates that he/she is the only one who has access to and will use his/her specific CAIS password. The agreement acknowledges the physician understands the electronic signature will be equivalent to a legal signature and understands the consequences of failing to comply with the agreement.
    - Encryption of passwords when stored or sent over the network.
    - Reporting of misuse of passwords to the medical professional practice leader.
    - Auditing of signature related actions by the Regional Medical Professional Practice leaders.

Procedure

1) The Agency will obtain, at the time of the Credentialling process*, a signed Electronic Signature and Password Confidentiality Agreement from physicians eligible for electronic signature authorization. Physicians eligible for the electronic signature authorization correspond to physicians who have doctor-in-charge privileges as outlined in the medical staff bylaws. The agreement will be maintained on the physician file.

2) *The agreement may be signed at the time temporary privileges are granted.

3) Procedures for forgotten passwords and password deletions will follow the Agency password policy requirements. IT will be responsible for maintaining electronic signature passwords on the network.

4) There will be a capacity for the Health Information Management to audit the electronic signature (Audit to include verification the document was routed to the Most Responsible Physician for

signature, opened and viewed by this physician and signed electronically (for documents requiring signature).

Appendix I

BRITISH COLUMBIA CANCER AGENCY
Electronic Signature and Password Confidentiality Agreement

Application of the Agency Cancer Information System (CAIS) password in conjunction with the electronic signature process will create the magnetic impulse, which I understand is equivalent to my written signature.

I understand it is essential the following guidelines be adhered to:

- The electronic signature is considered the legal equivalent to my handwritten signature or initials.
- I will not disclose my password to anyone, nor will I attempt to learn or use another person's (CAIS) password.
- If I have reason to believe that my CAIS password code has been revealed, I will immediately contact Information Technology to be issued a new code.
- I understand that any violation of the above, or any other misuse of my confidential password violates Agency policy and may be subject to legal and/or other actions by the Agency including loss of privilege of access to the Information System or dismissal.

(The Electronic Signature Policy PIM 020 requires signature of a password confidentiality agreement).

Name of Physician_____

Signature_____

Witnessed this _____ day of _____, 20 _____.

_____
Name

_____
Address