



University of Connecticut Health Center

POLICY NUMBER 2006-05

May 5, 2006

POLICY: ELECTRONIC SIGNATURE FOR MEDICAL RECORDS

PURPOSE:

To facilitate the usage of electronic signatures for medical records throughout the clinical operations of the Health Center.

POLICY STATEMENT:

Electronic signature, an automated function which replaces a handwritten signature with a system generated signature statement, will be utilized for medical records as a means for authentication of transcribed documents, computer generated documents and/or electronic entries. System generated electronic signatures are considered legally binding as a means to identify the author of medical record entries and confirm that the contents are what the author intended.

Providers will be allowed to utilize electronic signature in accordance with this policy and State and Federal regulations regarding such.

PROCEDURE:

1. **APPROVAL** - All electronic signature applications must be approved for use by the Health Information Management Committee with further approval by the Health Center's governing body as needed.
2. **ELECTRONIC SIGNATURES ALLOWED** – The following types of electronic signatures can be utilized:
 - Electronic signature statement (digital signature)
 - Digitized signature (actual signature converted to electronic image)

If the application allows auto-authentication or auto-signatures this functionality is prohibited. The author of the entry will be required to review/validate the entry prior to applying electronic or digitized signature.

3. **SECURITY**

- A. Confidentiality statement – Any provider authorized to utilize electronic signature will be required to sign a statement attesting that he or she is the only one who has access to his/her signature codes, that the electronic signature will be legally binding and that passwords and/or PIN numbers will not be shared (see Exhibit A).

- B. Passwords - All users will have their own user ID and password. Passwords must be at least six characters long and include at least one number or symbol. Passwords will expire every 90 days and must be reset. They can not be repeated for at least five cycles.
- C. Personal Identification Numbers (PIN)/ Secondary Passwords – PIN numbers and/or secondary passwords will be assigned when possible for use with electronic signatures to allow for another level of security.

PIN numbers or secondary passwords are not viewable on any screen.

- D. Before assigning the unique user name the system administrator shall verify the user (see HIPAA Security Manual – Access Control section for each applicable system).
- E. Providers who use electronic signature based upon the use of user IDs and passwords as described in this policy, shall use additional controls to ensure the security and integrity of each user's electronic signature:

- 1) Follow loss management procedures to electronically deauthorize lost, stolen, missing or otherwise compromised documents or devices that bear or generate identification code or password information and use suitable, rigorous controls to issue temporary or permanent replacements.
- 2) Use safeguards to prevent the unauthorized use or attempted use of passwords and/or identification codes; and
- 3) Test or use only tested devices, such as tokens or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered.

4. USAGE OF ELECTRONIC SIGNATURE

- A. Electronic signatures can be utilized within many clinical applications including, but not limited to:

- Radiology
- Anatomic Pathology
- Clinical Laboratory
- Dermatopathology
- Physician Order Entry
- Health Information Management
- Emergency Department
- Cardiopulmonary
- OB

- B. Providers are required to review their entries for completeness and accuracy prior to electronically signing them.

- C. Once an entry has been signed electronically, the computer system will prevent it from being deleted or altered. If errors are later found in the entry or if information must be added, this will be done by means of addendum to the original entry. The addendum should also be signed electronically and date/time stamped.
- D. The signature line of a document signed electronically will include either a digitized signature and/or a signature statement with the authenticator's name and date the document or entry was signed, time of authentication will also be provided depending on the system's capabilities. This will depend upon how each individual system is set up to handle electronic signature.
- E. System specific standards and procedures for usage may vary from system to system and it will be required that any department who utilizes electronic signature must establish and maintain system specific procedures for its use.
- F. Any misuse or disregard of electronic signature policy will be reviewed and acted upon by the Health Information Management Committee. Sanctions will be imposed if deemed necessary.

5. AUDITING ELECTRONIC SIGNATURE

Providers must use a secure, computer-generated, time-stamped audit trail that records independently the date and time of user entries, including actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information. Audit trail documentation shall be retained for a period at least as long as that required for the medical record and shall be made available as needed upon request.

Steven Strongwater, M.D. (signed)
Steven Strongwater, M.D.
Associate Dean for Clinical Affairs
Director of Clinical Operations

6/5/06
Date

Elena Albini, R.H.I.A. (signed)
Elena Albini, R.H.I.A.
Director of Health Information Management

6/5/06
Date

Peter J. Deckers, M.D. (signed)
Peter J. Deckers, M.D.
Executive Vice President for Health Affairs

6/5/06
Date

NEW POLICY: May 5, 2006