

Appendix M
SAMPLE ELECTRONIC SIGNATURE POLICY
(for a pen-based digital system for a home health service)

Electronic Signature Policy

[Name of Facility] has adopted this Electronic Signature Policy to comply with legal and accreditation standards requiring authentication of medical records and the Regulation's requirement to protect the security of electronic health information, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements.

Assumptions

- The Medical Records Committee of the Medical Staff has approved the use of electronic signatures to authenticate the entries in patients' medical records.
- Such electronic signatures are in accordance with federal and state law.
- The use of such electronic signatures are part of [Name of facility]'s overall security program.
- Misuse of the authentication process, as by sharing passwords and/or signature keys, pose significant risks to the integrity and confidentiality of patient and other confidential information.

Policy

All persons authorized to authenticate medical records must read, understand, and comply with this policy. In accordance with legal and accreditation standards and the authorization of the Medical Records Committee of the Medical Staff, [Name of facility] permits practitioners to authenticate entries by executing an electronic signature.

[Name of facility] uses a pen-based computer system that creates an electronic image of the practitioner's handwritten signature created by using a pen computer attached to or associated with an electronic record to authenticate the record.

The pen-based computer system, [name of system], provides a platform for the individual clinicians to "sign" by creating an electronic image of the clinician's individual handwritten signature.

- The Medical Records Committee is responsible for developing procedures for determining what individuals are authorized to authenticate particular portions of patient medical records.
- The clinician placing the electronic signature into the specified field(s) of the [name of system] system is considered to have signed and authenticated that specified information entered into the [name of system] system as a part of the patient's legal medical record.
- [Name of facility] provides the clinical staff training and orientation on the use of the electronic signature as a required part of training on the automated medical record.
- The signature applied within the automated medical record system is considered the authentication of the specific entry into the medical record, whether that electronic signature image is reviewed on a workstation or pen-based tablet screen directly within the computerized medical record system, or whether the signature image has been printed on the paper version of the visit note or medical record entry.
- Clinician staff applying the electronic signature are attesting to having reviewed the contents of that entry and having determined that the entry contains what the individual clinician intended. Once the clinician has authenticated the entry, the system does not permit anyone to overwrite, delete, or alter it. Corrections must be made by generating a new entry.

[Name of facility]'s security system protects the pen-based computer system by two levels of access control mechanisms with unique identifiers being assigned to each individual user on the system.

- To gain entry into the [name of system] on the pen-based tablet unit and access patients' medical record information, the clinician must authenticate him or herself on two levels:
- After turning on the pen-based tablet unit, a unique login and password specific to the clinician must be entered to gain access to the applications on the tablet unit.
- To enter the specific [name of system] system on the tablet, a second unique login and password specific to the clinician must be entered to gain access to patient information.
- Once the clinician has authenticated into the patient information area of [name of system] system, only patients assigned to that clinician during scheduling or case management assignment are available to that clinician on the tablet.
- The tablet will reject a user and deny entry into the [name of system] patient system after three (3) attempts at entering the unique login and password information incorrectly. System Administrator level intervention is required for the clinician to gain access into the system. System Administration level access is granted only to the System Administrator and specific controlled designees who have been trained in system security policies and procedures. This prevents unauthorized entry into the secured patient medical records and ensures that only appropriately identified and password-secured staff access secured patient areas of the system.
- Passwords are unique to the clinicians. Clinicians may not share their login or password information and must treat it as strictly confidential.

To further safeguard against unauthorized access to the system and forgery of electronic signatures:

- Tablets are locked in the network server room when not issued to a clinical staff.
- Each individual clinician is assigned a specific tablet with a number unique to that clinician.
- Clinicians may not use another clinician's tablet, and do not have login or password access to use another clinician's tablet. The system will deny access to that tablet should he or she attempt access.
- [Name of facility] assigns patients to clinician's tablets only when that clinician is case managing the patient or scheduled to make visits to the patient. Access to electronic medical records is restricted to clinical staff actually providing care or involved in the case management of the patient.
- The System Administrator maintains the assignment of tablets, logins, passwords, and tablet numbers. Only specifically designated staff may perform those tasks under the supervision of the System Administrator in accordance with [Name of facility]'s Security Policy.
- Entries onto the tablet that the clinician has electronically signed are locked, and cannot be altered by the clinician or other staff member.
- Medical record entries that are locked can only be unlocked by the System Administrator level staff, only in specific circumstances for corrections not related to the content of the medical record, and such unlockings of the medical record are recorded in the audit trail records.
- The system maintains an audit trail providing details of user names accessing medical records and/or unlocking medical records.

[Name of facility] will maintain hardware, server, and network security consistent with its Security Policy.

- The server for the [name of system] is maintained in the secured server network room of the department with access restricted to authorized staff per the Security Policy.

- The server for the [name of system], including patient data, is included in the virus protection, daily back-up, disaster plan, recovery, and general network security provisions of [Name of facility]’s Security Policy.

[Name of facility] will train and educate staff in the proper use of the electronic signature.

- All clinical staff using the pen-based units for patient documentation must attend security training on the unit, protection of confidential data, and maintaining closed access to the unit. Remote access to the unit is not permitted.

- Clinical staff must sign the Equipment Release document after they have attended the educational session on patient information security policies and maintaining confidentiality of the system to protect patient data.

- [Name of facility] will instruct clinical staff on the facility’s progressive disciplinary policy and that failure to adhere to all required security processes will result in disciplinary action.

- [Name of facility] will configure pen-based units issued to clinical staff to permit only dialing into and transmission of patient data to [Name of facility]’s [name of system] NT Server.

- Any attempt by staff to alter the dial-up configurations (such as by, Internet access), will result in disciplinary action.

- The System Administrator will periodically monitor pen-based units for any configuration alterations.

- Support and administrative staff access and training.

- Only specific clinical staff have access rights to make an electronic signature entry into a secured area of a patient medical record. Support staff and administrative staff logins do not permit them access to entering or altering electronic signatures or patient data in the system.

- Support and administrative staff are also required to sign the Equipment Release document before using the [name of system] and also receive training in and review of the Network Security Policy to ensure patient confidentiality on the workstations.

Enforcement

All supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment in accordance with the facility’s Sanction Policy.

Portions of this Policy were adapted from the Electronic Signature Policy of Home Health Services of Southwest General Health Center.

Appendix