Policy: ELECTRONIC SIGNATURE, ATTESTATION, AND AUTHORSHIP FOR MEDICAL RECORD DOCUMENTATION

ORGANIZATIONAL: Effects two or more departments.							
Folder	Organizational Choices: Health Information Mgmt			**Sub-Folder** (If Applicable)	**n/a**		
Original Effective Date	11/1/2011	**Scope**	*What departments does this policy apply to? State "All" as is may apply to the entire organization.* *All clinicians who document in the medical record; HIM staff; medical staff services staff*				
Approved (Approver/Date)	MDRC: 7/2019						
Last Reviewed/ Revised Date	7/30/2019	**OSHA Category** (If Applicable)	Not Applicable	**Standard** (If Applicable)	*RC 01.02.01*	**Number of pages**	5

PURPOSE: *Why does this policy exist?*
To improve signature legibility, facilitate the use of electronic signatures for health records generated during healthcare operations, validate information accuracy and completeness, verify the identification and appropriateness of electronic health record authors, and support nonrepudiation through the use of legal and compliant electronic signatures.

GUIDELINES: *What are some general statements regarding the use of the policy?*
Electronic signatures are used on health records as a means of attestation of electronic health record (EHR) entries, transcribed documents, handwritten entries, and computer-generated documents. Properly executed electronic signatures are considered legally binding as a means to identify the author of health record entries, confirm content accuracy and completeness as intended by the author, and to ensure e-signature integrity is maintained for the life of the electronic health record.

Electronic signature, attestation, and authorship are referred to in this document as *e-signature*. Individuals authorized to affix an electronic signature to medical record documentation shall be limited to individuals with defined privileges to document in the medical record (see *Authorization to Document in the Medical Record* policy on Policy Manager).

It is the policy of Southeast Hospital to accept electronic signatures as defined within this policy for author validation of documentation, content accuracy and completeness with all the associated ethical, business, and legal implications. This process operates within a secured infrastructure, ensuring integrity of process and minimizing risk of unauthorized activity in the design, use, and access of the EHR.

PROCEDURE: *Include: Definitions , Equipment , Process, and Documentation*

Definitions

Attestation – the act of applying an electronic signature to the content, verifying accuracy of documentation content, showing authorship and legal responsibility for a particular unit of information.

Authentication – the security process of verifying a user's identify with the system that authorizes the individual to access the system (i.e., sign-on process). Authentication shows authorship and assigns responsibility for an act, event, condition, opinion, or diagnosis.

Authorship – attributing the origination or creation of a particular unit of information to a specific individual or entity acting at a particular time.

Electronic signature – a generic, technology-neutral term for the various ways that an electronic record can be signed, including a digitized image of a signature, a name typed at the end of an email message by the sender, a biometric identifier, a secret code or PIN, or a digital signature.

Data Elements Required in E-Signatures

The e-signature line includes the author's e-signature, full name, credentials, date, and time of e-signing.

Special Considerations for E-Signatures

Variation in technology implemented and services offered may require policy coverage of multiple provisions for special e-signature practices. Policy defines the necessary approaches and approved functionalities.

1. Electronic Dual Signatures, Co-Signatures, and Counter-Signatures

Entries or reports containing documented contributions by multiple individuals must be authenticated by each contributor in a way that unambiguously identifies each individual's specific contribution. Multiple signatures are applicable to a single entry or document where required by institutional policy (see Rules and Regulations in the Medical Staff Guidelines). When applied, each signature should be complete for required elements. Transcribed reports as well as medical record entries must show the name of the dictator and/or person entering medical information, as well as display the names of all e-signers. The sequence of e-signature applications must be evident within the metadata. HIM staff will monitor compliance with this to ensure record integrity is maintained.

2. Proxy, Alternate, or Group Signatures

The process by which another provider is authorized to electronically sign documentation on behalf of the original author in an ongoing manner. The proxy accepts responsibility for the content of the original documentation.

3. Auto-Attestation

Auto-attestation is the process by which a physician or other practitioner authenticates an entry that he or she has not reviewed or cannot review because it has not yet been transcribed or the electronic entry cannot be displayed. This process is ***strictly prohibited*** as a method of authentication in a health record.

4. Dictation Disclaimers

Utilizing a disclaimer to the effect that documentation was created with voice-recognition technology/errors can be expected or was dictated but has not been read is ***strictly prohibited*** (please see *Provider-Created Documentation QA* policy on Policy Manager).

Electronic Signature Participation

This policy includes reference to the conditions under which an individual is required or given permission to participate in the e-signature process. Individuals responsible for documenting in the electronic medical record shall complete the ***Request for Authorization to use an Electronic Signature*** form contained within the *Medical Staff and LHP-A Application* supplied by Medical Staff Services (see Appendix A).

1. Confidentiality and Security

Participant agreement – each e-signer is required to complete a participation agreement attesting to be the only person with access to the identifier, code, password, or PIN with commitment to safekeeping of user information. The agreement provides acknowledgement of and user intention to uphold organization policies and practices for a properly executed e-signature process. Retention responsibilities for the completed agreements are retained by Medical Staff Services.

Participant identification – those authorized to affix an electronic signature will be limited to those identified by policy, such as treating physicians, other clinicians, ancillary healthcare staff, and clinical residents and students involved in patient care requiring record documentation and/or review and approval of documentation in the health record.

Security – robust organization technological security safeguards create the foundation of the e-signature functional design. Safeguards to enhance and afford the reliability of e-signature functions are carefully selected and updated as technology advances. Under no circumstances may users provide any other person, including physician office staff, other physicians, or family members access PIN or e-signature functionality. All users of electronic signatures must comply with confidentiality requirements outlined in the facility-wide policies on confidentiality and security of health information. Any security breach such as problems with passwords and/or PINs must be promptly dealt with and changed if they are suspected or known to have been compromised.

System authentication – a PIN, password, or other measure should be used to identify each authorized user. This PIN or password should be confidential, known only to the user, and adequately complex by security best practices and organizational policy (see Organizational Password Selection).

2. Compliance Monitoring

The HIM department will be responsible for ensuring that medical records are authenticated and the charts completed within the timeframe delineated in hospital policy and Medical Staff Bylaws/Rules and Regulations. Please refer to the *Medical Record Deficiencies and Voluntary Relinquishment of Privileges* and *Filing a Record Incomplete* policies located in Policy Manager, as well as the Medical Staff Rules and Regulations, for further details.

3. Enforcement/Disciplinary Action

The enforcement and sanctioning models adopted are administered in a fair, consistent, and objective manner.

Any individual who makes inappropriate or illegal use of electronic signatures or records is subject to policy enforcement and disciplinary sanctions. Sanctions, based upon the signatory's relationship with Southeast Hospital, may include professional review, suspension, revocation of privileges, termination of employment, and criminal prosecution.

Inappropriate or illegal use includes but is not limited to anyone who discloses his or her PIN or password to others and anyone using a PIN or password of another without authorization.

REFERENCES: *What resources are used to support the policy and procedure?*

LaTour, K. M., Eichenwald Maki, S., & Oachs, P. K. (2013). *Health information management: Concepts, principles, and practice* (4th ed.). AHIMA Press: Chicago, IL.

Southeast Health Medical Staff Rules and Regulations, Revised 2015

Southeast Hospital policy – Authorization to Document in the Medical Record

Southeast Hospital policy – Filing a Record Incomplete

Southeast Hospital policy – Medical Record Deficiencies and Voluntary Relinquishment of Privileges

Southeast Hospital policy – Provider-Created Documentation QA

Attachments: (Label as Appendix A, B, C, etc.)

Appendix A

Request for Authorization to use an Electronic Signature:

The use of electronic signatures is an approved method of signing medical record documentation by Medical Staff Members and Limited Health Practitioners–Advanced (LHP-A) at Southeast Health. Utilization will be authorized through combined efforts of Health Information Management (HIM) and Information Systems upon completion of the authorization, request and attestation that appear below.

Attestation:

1. My electronic signature PIN is the equivalent of my signature as recognized by Southeast Health, the State of Missouri, and (The Joint Commission) TJC.
2. I am the only one who has access to and will use my electronic signature PIN. I will not give the PIN to anyone else or let anyone else use it.
3. I will not learn or use anyone else's electronic signature PIN.
4. I will not access or attempt to access unauthorized information.
5. I will review all medical record entries for completeness and accuracy and make corrections or modifications as needed. All copies of a document that result from correction or addendum to a document will remain as part of the permanent medical record.
6. Misuse of my electronic signature PIN may result in termination of my access to electronically sign all my documentation.
7. Reviewing and finalizing a document will result in this statement, "This document was electronically signed by (*Name of Medical Staff Member/LHP-A* on (*this date*) at (*time*)."

Request: I authorize and request that my signature be affixed to all my medical record entries and dictated reports following my review according to the electronic signature policy which has been provided to me and I have read. The PIN provided to me by Information Systems will be considered my E-Signature. I will adhere to the above guidelines in utilizing my electronic signature.

_____

Signature Date