Electronic Signature, Attestation, and Authorship.

Appendix C: Electronic Signature Model Policy
This template document is not intended for adoption as a substitute for a customized organizational policy of specificity and action steps appropriate to local factors.

Advancing technology and changing surveillance criteria make any technology adaptation an evolution. An applied and reputable approach will balance front-end technology capabilities against back-end administrative controls to measure compliance.

Development of an electronic signature policy is an important aspect of a healthcare organization's legal electronic health record definition. AHIMA recommends legal counsel review the policy during the approval process. If technology limitations preclude implementation of optimal electronic signature approaches, organizations should identify gaps for future technology acquisitions and workflow improvements.

This model policy template recommends important legal and compliance considerations for healthcare organizations' electronic signature policy and procedures. An appropriate organizational policy reflects best practices along with germane international, federal, and state laws and regulations, accreditation standards, payer requirements, documentation requirements for clinical services offered, and technology functionalities.

Term definitions in this document are taken from the glossary in appendix D. They are intended to be used together.

Subject/Title Electronic Signature, Attestation, and Authorship for Medical Record Documentation
Page 1 of X

Revision History
Effective Date: xx-xx-xx
Departments Affected:
Health Information Services/Management, Medical Staff, Nursing, Ancillary Healthcare Providers, Human Resources
Original Issue Date: xx-xx-xx
Last Reviewed: xx-xx-xx
Last Revision: xx-xx-xx

Purpose: To establish a foundation for technical and human interaction policy and procedure decisions to guide legal and compliant electronic signature processes. To improve signature legibility, improve record completion timeliness, 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.

Scope: Electronic signature, attestation, and authorship are referred to in this document as *esignature*.
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, such as treating physicians, other clinicians, ancillary healthcare staff, and clinical residents and students.

Policy Statement: Electronic signature is used for health records as a means of attestation of electronic health record entries, transcribed documents, 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.
It is the policy of the healthcare organization 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 electronic health record.

Definitions

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

Authentication: the security process of verifying a user's identity with the system that authorizes the individual to access the system (i.e., the 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.

Policy
The policy defines the components and elements that make up the healthcare organization's approved approach to e-signature.

1. Electronic Signature Authentication

a. General Principles
Current laws and regulations (international, federal, and state), accreditation standards, and payer and local policies and requirements are taken into account in developing organizational policy to ensure compliance at all levels.

E-signature policy is set by a multidisciplinary group or committee knowledgeable in the laws, technology, ethics, and best practices, such as those identified in the approvals signature section at the end of this document. A carefully defined approvals protocol ensures concurrence by all positions and areas responsible for establishing and maintaining a reputable approach to electronic signature.

New EHR software acquisition decisions include due diligence to assess functional capability to uphold the organization's e-signature requirements.

Periodic software updates and upgrades include pre-implementation investigation and testing of design differences or changes impacting a valid, legal approach to e-signature. As technology and software improvements strengthen the e-signature process, policy, and procedure, documents are updated and staff training carried out.

Verification of content accuracy and completeness of each entry or document is made by the author prior to attestation.

An e-signature event captures and displays the e-signature, author's name, credentials, date, and time of application.

Once an entry has been electronically signed, the system prevents deletion or alteration of the entry and its related electronic signature for the life of the referenced documentation.

The policy addresses an organization's acceptable timeliness parameters related to an e-signature application. Factors such as germane laws, regulations, accreditation standards, and operational factors would be considered in an organization's definitions.

Up-to-date policy and procedures are readily accessible by all e-signature users. Staff communication and training includes timely updates of policy and procedural changes.

The policy addresses acceptability of imported electronic documents with an e-signature component into the EHR and legal health record. If the type and method of e-signature on an external document is a decision-making factor to allow import of a document, the e-signature policy addresses its alignment with the organization's separate policy for management of external documents.

b. Types of E-Signatures

The policy delineates the types of e-signature functionality acceptable for use in the organization and the method of organization approval of each type prior to initial use.
A properly executed electronic process signifying an approval of an entry or document content presented in electronic format may encompass a broad gamut of technologies and methodologies, ranging from an "I agree" button in a click-through agreement, to an electronic tablet that accepts a handwritten digitized signature, to a digital signature cryptographically tied to a digital ID or certificate.
An electronic signature approach or proposed software design is formally approved by a

multidisciplinary body prior to first use, such as the medical record committee or an EHR governance committee. A written proposal accompanied by a functional demonstration is recommended as part of the investigation and approval process.
Acceptable and approved functional types may include:

Biometric: use of biological data**,** such as fingerprints, handprints, retinal scans, and pen strokes, to authenticate an individual.

Digital signature: a cryptographic signature (a digital key) that authenticates the user, provides nonrepudiation, and ensures message integrity. This is the strongest signature because it protects the signature by a type of "tamper-proof seal" that breaks if the message content was to be altered.

Digitized signature: an electronic representation of a handwritten signature. The image of a handwritten signature may be created and saved using various methods, such as using a signature pad, scanning a wet signature, or digital photography. The signature may be "captured" in real time (at the time the user applies the signature), or a saved image captured at the point of normal business operations may be imported. The digitized signature is useful for patient signatures that must be collected for admission consent, surgical consent, authorizations, discharge instructions, advance directives, and generally any other type of electronic form requiring patient signature.

c. Data Elements Required in E-Signature

Policy defines the screen visual and hard-copy appearance of the applied e-signature for user and legal identification.
The e-signature line includes the author's e-signature, full name, credentials, date, and time of e-signing.
Accompanying signature phrases approved and acceptable for EHR authentication statements are identified. Phrases selected should be fitting to the type of documentation referenced. Examples include "Electronically signed by"; "Signed by"; "Authenticated by"; "Sealed by"; "Data entered by"; "Approved by"; "Completed by"; "Verified by"; "Finalized by"; "Validated by"; "Generated by"; and "Confirmed by."

d. Amendments, Corrections, Deletions, and Retractions in the EHR

Policy defines the provider's electronic approach to amendments, corrections, deletions, and retractions in keeping with legal principles. Any necessary revisions to an electronically signed document must follow organizational policy and procedure. These changes require the same data elements described in the "Types of E-Signatures" section. Please refer to two toolkits, "Amendment, Corrections and Deletions Toolkit" and Amendments, Corrections, and Deletions in Transcribed Reports Toolkit," for recommended procedures.

Addendum: new documentation *added* to original entry. Addendums should be timely and bear the current date and reason for the additional information being added to the health record.

Amendment: documentation meant to *clarify* health information within a health record. An amendment is made after the original documentation has been completed by the provider. All amendments should be timely and bear the current date of documentation.

Correction: a *change* in the information that is meant to clarify inaccuracies after the original documentation has been signed or rendered complete.

Deletion: the act of *eliminating* information from previously closed documentation without substituting new information.
Late entry: delayed EHR documentation. The entry pertains to the regular course of business for the patient it addresses but is recorded subsequent to the usual and customary point-of-care documentation timeliness. The delay often creates documentation sequencing outside of normal chronological order.
Retraction: the act of correcting information that was inaccurate, invalid, or made in error and preventing its display or hiding the entry or documentation from further general view**.** After an entry or document has been invalidated, it must be retained in a retracted state in the version control portion of the legal health record for access if needed for legal or other purposes. Organizational policy should provide guidelines on when a correction is made versus retraction.

2. Special Consideration for E-Signature
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.

a. Electronic Dual Signatures, Cosignatures, and Countersignatures
Definitions of the three synonyms**:** Additional or supplemental signature(s), electronically affixed, in those instances where state or federal law, academic teaching programs, facility guidelines, or clinical preference call for multiple attestations on a particular unit of information.
For example, a resident may dictate, edit, and sign a document to indicate authorship. The responsible supervising physician may be required to sign the document in addition to the resident. Recommended e-signature practices for dual signatures, cosignatures, and counter signatures are included in the toolkits "Amendments, Corrections, and Deletions in the Electronic Health Record Toolkit" and "Amendments, Corrections, and Deletions in Transcribed Reports Toolkit."
In the case of transcribed documents, the point at which the e-signature is affixed is the point at which the document is locked for editing changes. After e-signing, the amendments, corrections, and deletions procedures are employed.

b. Entries Made on Behalf of Another

At the point of care. If documentation of care is recorded by one individual for another when both are present, such as in a scribe role or an emergency trauma or code event, the e-signature capture should include identifying information of both individuals. At a minimum, the identification of the person who documented the information, the date, and time should be captured, along with an attestation e-signature of the ultimately responsible caregiver noting corresponding date and time of attestation. Title identity should be clearly noted respectively for each e-signature (e.g., scribe versus caregiver).

For final health record completion. In the event a physician or other clinical provider is protractedly absent leaving unsigned electronic documents or entries, a process is in place to invite qualified alternate signers for purposes of record closure. A qualified alternate

signer is one who is able to uphold the purpose of attestation, that of familiarity with the clinical case that can validate the accuracy of the documentation. When entries must be left unsigned due to case unfamiliarity by other caregivers and lack of alternate signers, explanatory documentation is included in the EHR to indicate the reason for record closure with e-signature validation gaps.

c. 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. The use of proxy signature technology should be monitored to ensure the purpose of e-signature is upheld.

d. Multiple 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. When applied, each signature should be complete for required elements. Transcribed reports must show the name of the dictator as well as display the names of all e-signers. The sequence of e-signature applications must be evident within the metadata.
.

e. Auto-attestation
Auto-attestation is the process by which a physician or other practitioner authenticates an entry that he or she 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.
The method used to apply an electronic signature must promote action by the signer to verify the entry or report content displays as intended and the information is accurate.

f. **Patient and Witness Signatures**
Documents requiring patient or witness signature are part of the patient's legal health record. Approaches to legal patient and witness signatures may include electronic signatures such as digitized handwritten signature and digital signature. The same principles for uninterrupted security and guarantee of unalterable functionality apply.

3. Electronic Signature Participation
The policy includes reference to the conditions under which an individual is required or given permission to participate in the e-signature process.

a. Confidentiality and Security

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. Authorized titles are documented in medical staff bylaws or rules and

regulations and organizational policies and procedures.

Security: robust security technological safeguards create the foundation of the e-signature functional design. Technology fortifies the reliability of signature functions that 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 (e.g., patient or witness users) access to user ID, 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, two-factor, multifactor, or biometric authentication, and access ID codes and PINs must be promptly dealt with and changed if they are suspected or known to have been compromised.

System authentication: a unique ID number, code, password, or other measure such as fingerprint or voice activation code should be used to identify each authorized user. This ID, code, or password should be confidential, known only to the user, and adequately complex by security best practices and organization policy.

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 acknowledgment of and user intention to uphold organization policies and practices for a properly executed e-signature process. Retention responsibilities for the completed agreements and signing frequency practices are described; for example, requiring that a provider signs an initial agreement prior to first use, with annual agreement renewal thereafter. The agreement can be retained by the health information management department, medical staff office in physician profiles, or human resources department in employee files.

b. Compliance Monitoring

The policy designates requirements for planned compliance monitoring in the form of ongoing or periodic audits to measure participant alignment with policy and procedure expectations and detect inappropriate e-signature practices whether from ignorance, negligence, or overt policy abuse.

Unannounced ongoing audits should be part of the organization's performance improvement program. The approach includes a check-the-checker provision, one that recognizes the accuracy of the evaluator should also be checked periodically.

More frequent back-end compliance monitoring with larger sample size may be needed to offset front-end technology limitations in order to adequately measure compliance.

c. Enforcement/Disciplinary Action

The policy identifies alignment with the organization's existing enforcement and disciplinary policies.

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 the healthcare facility, 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 ID number, code, or password to others, and anyone using a PIN or ID number, code, or password without authorization.
A tiered sanctions approach to inappropriate participant actions is recommended.
Please refer to AHIMA's practice brief "Sanction Guidelines for Privacy and Security Breaches."

Procedure Development

General Principles
Step-by-step procedural details and staff instructions must be created to support the technology and policy approaches, components, and elements identified and approved.
The procedure should be developed by individuals knowledgeable of policy requirements, ethics, and technology functions and limitations.
Detailed procedure specifics should be adequate and intuitive for participant understanding and ongoing reference. Documents such as these may also be requested by surveillance bodies such as the Office for Civil Rights for compliance assessments and Joint Commission for accreditation surveys.
Procedure documentation may require multiple separate documents or procedural subsections to accommodate disparate e-signature approaches when multiple technology system functionality sets are in place. Distinct procedures may also be helpful for customized training of different participant groups.

Approvals
Appropriate policy approvals are evident and legible on the documented policy, such as:
Executive Approval:
Date:
Medical Staff Approval:
Date:
Health Information Management Approval:
Date:
Compliance/Risk Management Approval:
Date:
IT Department Approval:
Date:
Legal Council Approval:
Date: