Electronic Signature, Attestation, and Authorship (2009 update) - Retired

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Editor's note: This update supplants the October 2003 practice brief "Implementing Electronic Signatures."

Electronic health record (EHR) systems provide the ability to sign entries electronically; however, implementing and using e-signatures is complex. This practice brief provides insight into the technology used to implement e-signatures, the related health IT standards, the regulatory environment, and recommendations on best practices.

This online version of the practice brief provides additional e-signature resources, tools, a glossary, and best practices to assist HIM professionals with EHR implementation and policy development.

While this practice brief addresses an organization's internal approach to determining e-signature policy and procedures, the foundational principles should extend beyond an organization's operations to external health information exchange efforts and participation agreements with HIE partners. As the healthcare industry evolves, an HIE's business plan and supporting functions must include valid, legal, consistent, and agreed-upon e-signature methods of nonrepudiation for use by all participants.

An Evolving Definition of E-Signature

The EHR has changed certain concepts and terms related to signatures. In the past, HIM professionals identified the act of signing an entry as authentication. However, this definition has evolved.

In EHRs, **authentication** is the security process of verifying a user's identity that authorizes the individual to access the system (e.g., the sign-on process). Authentication is important because it assigns responsibility to the user for entries he or she creates, modifies, or views. **Attestation,** on the other hand, is the act of applying an e-signature to the content, showing authorship and legal responsibility for a particular unit of information.[1]

Signatures, like medical records, can be either **analog** (e.g., stored on paper and unable to be read by a computer) or **digital** (e.g., stored on electronic media such as disks that can be read by a computer). The term *electronic signature* is frequently used in references and regulations in reference to signatures in a digital format. However, an **electronic signature** is a generic, technology-neutral term for the various ways that an electronic record can be signed (attested). It can include a digitized image of a signature, a biometric identifier, a secret code or PIN, or a digital signature.

Regardless of the type used, a signature serves three main purposes:

- **Intent:** an electronic signature is a symbol that signifies intent such as an approval of terms, confirmation that the signer reviewed and approved the content, or the signer authored the document and approves the content.
- **Identity:** the signature identifies the person signing.
- **Integrity:** a signature guards the integrity of the document against repudiation (the signer claiming the entry is invalid) or alteration.[2]

In EHRs, e-signatures encompass a broad range of technologies and methods, ranging from an "I agree" button in a clickthrough agreement, to an electronic tablet that accepts a handwritten signature, to a digital signature cryptographically tied to a digital ID or certificate.

Signature mechanisms that are typically found in EHRs today are listed in the sidebar at right. In today's environment, the type of individual software application drives the production of clinical documentation in the medical record, therein also driving the method and applicability of e-signatures. Limitations of an individual system's requirements and the flexibility of how those signatures are applied will continue to depend on system specifics for these applications.

Laws, Regulations, and Electronic Signature Acts

Since the advent of fax machines, handwritten signatures have been accepted electronically. With the rise in technology, there has been an influx of laws and regulatory agencies providing standards for use of e-signatures.

However, there is no single overwhelmingly accepted standard, law, or regulation, and organizations must access individual resources to review existing language specific to e-signatures, attestation, and authorship of medical record documents in an EHR. Unfortunately, these sources may contradict one another, making it even more difficult for the organization to determine its policy.

For summarized information on these laws, regulatory agencies, and their rules on electronic standards or use, including links to Web sites, refer to appendix B "Laws, Regulations, and Electronic Signature Acts."

Typical E-Signature Mechanisms

Signature mechanisms typically found in EHRs today are listed below in order of their strength—level 1 is the weakest, and level 3 the strongest.

Level 1—Digitized Signature: an electronic representation (applied image) of a handwritten signature. The image may be created by various methods, such as 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 previously saved image may be applied. A digitized signature is the weakest form of e-signature because someone could acquire a copy of the image of the handwritten signature and forge an electronic document.

Digitized signatures are often used for documents such as patient consents, agreements, and authorizations. They may also be used or preferred for documents that are printed and shared with physicians outside the healthcare organization, particularly for transcribed documents such as consultations and letters that are distributed to referring physicians. Organizations should develop policies to ensure readability and identification of the signer of digitized signatures.

Level 2—Button, PIN, Biometric, or Token: a frequently used e-signature methodology in EHR systems includes clicking a button or entering a unique personal identification number (PIN), electronic identification, token, or biometric scan at the completion of an entry for the signature process. EHR systems and organization policy should require some action that represents this signing process, such as pushing an attest button.

To strengthen the signature (which in turn strengthens the integrity of the record), healthcare organizations can add more tiers of security to the signature, such as a unique PIN, biometric, or digital signature. Strengthening the signature process minimizes the risk that an individual can refute the validity of the entry.

Level 3—Digital Signature: a digital signature is 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 were to be altered.

Nonrepudiation serves to protect the integrity of the document. It guarantees that the source of the medical record documentation cannot later deny that he or she was the author. Nonrepudiation may be achieved through the use of a digital signature, which serves as a unique identifier for an individual (much like a written signature on a paper document); confirmation service, which uses a message transfer agent to create a digital receipt (providing confirmation that a message was sent or received); and time stamp, which proves that a document existed at a certain date and time.

A digital certificate may be implemented as part of a digital signature. A digital certificate is an electronic credit card with attendant end-to-end security safeguards that establish a user's credentials when doing business or other transactions on the Web. It is issued by a certification authority and contains the user's name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Some digital certificates conform to the X.509 standard, published by the International Telecommunication Union. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.

Joint Commission Accreditation Standards

The Joint Commission accepts the use of e-signatures in hospitals and ambulatory care facilities, according to standard RC.01.02.01 in the *2009 Accreditation Manual for Hospitals and Ambulatory Care Facilities*.[3] The elements of performance require that:

- Only authorized individuals make entries in the medical record.
- The hospital or organization defines the types of entries in the health record made by nonindependent practitioners that require countersigning, in accordance with law and regulation.
- The author of each medical or clinical record entry is identified in the health record.
- Entries in the health record are authenticated by the author. Information introduced into the medical record through transcription or dictation is authenticated by the author.
- The individual identified by the signature stamp or method of electronic authentication is the only individual who uses it.

The Joint Commission also accepts the use of e-signatures in home care, long-term care, and mental health, subject to the requirements outlined above.

Payer and Health Plan Requirements

In addition to regulations, laws, and accreditation standards, payers and health plans may also require the use of e-signatures. Organizations should check payer requirements, local policies, and transmittals to determine the acceptability of e-signatures, technology requirements (such as digital signature technology), and specifications or limitations of use.

Health IT Standards for E-Signatures

Since there is no single overarching accepted standard for e-signatures, organizations must access individual health IT standards, regulations, and laws to review existing language specific to e-signatures, attestation, and authorship of medical record documents in an EHR. As general interoperability of systems improves over time, consistent standards will also be developed that can be applied to e-signatures.

Consistency and standardization is necessary. Users should be cognizant of the variability of existing standards, the ever-changing nature of such standards, and the various standard groups to remain up to date on current protocols and best practices.

Some of the standards that organizations can reference include:

- HL7 EHR-System Records Management and Evidentiary Support Functional Profile Standard. Health Level Seven developed the EHR-System Records Management and Evidentiary Support Functional Profile Standard, available in appendix A online, which identifies system functionality and conformance criteria related to authentication, attestation, pending records, amendments, and version management. Highlights from this standard for attestation include the need to link content to the authors, identify all authors or contributors of an entry, and display the name and credentials of authors.
- ASTM E1762–95(2003)–Standard Guide for Electronic Authentication of Health Care Information. ASTM International developed a standard in 2003 that outlines the appropriate process for applying an electronic signature, which involves

securely identifying the individual's identity and frequency, creating a logical manifestation of a signature, and ensuring the integrity of the signed document. The standard provides guidance on handling multiple signatures and signature attributes (e.g., time stamp, signature purpose, and signer's role).

- ISO/IEC 14888-3 Information Technology–Security Techniques–Digital Signatures with Appendix. This ISO standard specifies principles and technical requirements for digital signatures and the related cryptographic techniques including integer factoring, discrete logarithm, and constructing the message.
- Certification Commission for Healthcare Information Technology. Although not a standards organization, CCHIT develops certification criteria for EHR applications that draw from existing health IT standards. The 2009 ambulatory care EHR certification criteria require that systems have the ability to finalize a note and change the status of the note to complete so subsequent changes are recorded as such; record the identity of the user finalizing the note and the date and time; handle cosignatures; addend or correct a finalized note; provide the full content of the original and modified note; and identify the author of the change.

Workflow Process for E-Signatures

It is equally important to understand the workflow process related to e-signatures. The diagram [below] identifies the recommended process flow for e-signatures, including the need to collect all authors and complete a new version of the document or entry if there is a change after signature.

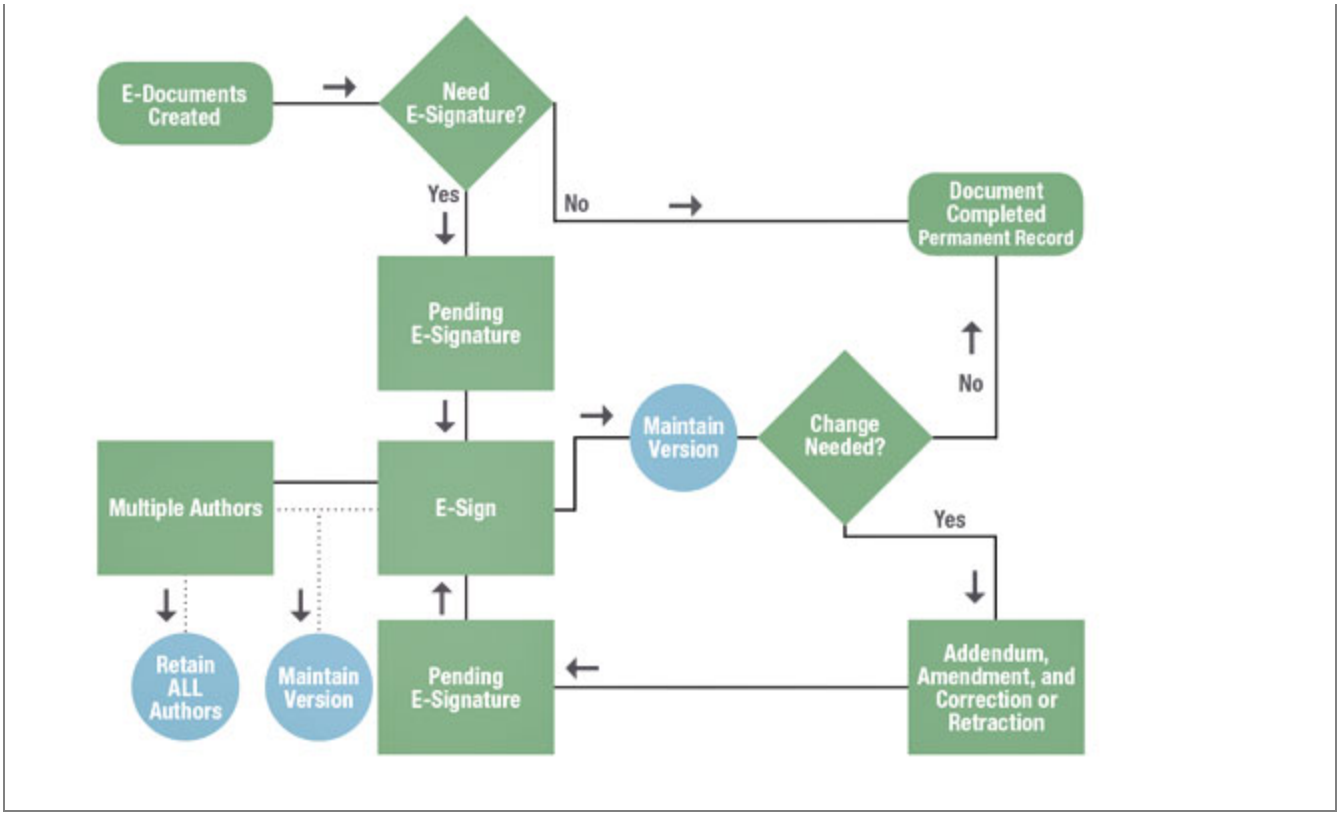
Implementation of E-Signatures in EHR, Electronic Document Management, and Transcription Systems

Healthcare organizations may implement e-signature functionality in a number of electronic record systems that include EHR applications, electronic document management systems, and transcription systems.

The different application of e-signatures has been a source of confusion for HIM professionals because implementation issues, workflow, and procedures differ between systems commonly used for EHRs. If an organization uses different types of systems, HIM professionals must understand the application of e-signatures in each of them. Policies and procedures should specify the application and applicable processes because e-signatures must be appropriately applied in all systems.

E-Signature Workflow Process

The diagram below identifies the recommended process flow for e-signatures, including the need to collect all authors and complete a new version of the document or entry if there is a change after signature. It follows the process from document creation through the various e-signature processes and to document completion. Solid lines represent the workflow. Dotted lines indicate system activity behind the scenes.



Authorship and Signature Special Considerations

Authorship attributes the origination or creation of a particular unit of information to a specific individual or entity acting at a particular time. While this concept seems fairly straightforward, authorship issues can arise in certain situations. Organizations should consider the following issues when developing their e-signature policies.

Multiple, dual, co-, and counter signatures. When there are multiple authors or contributors to a document, all signatures should be retained so that each individual's contribution is unambiguously identified. Care should be taken not to overwrite any author signatures on a document. Each signature should be complete and retained according to the organization's legal health record policy. Transcribed reports must show the name of the dictator and display the names of all electronic signers. The order of application of each signature must be provable via date and time stamps or other unambiguous means.

Entries made on behalf of another. Organizations must consider what procedures they will take when authors cannot or do not attest a document because they are no longer available to sign (e.g., resignation, sabbatical, or death). In the event a physician or other clinical provider is gone for an extended absence, leaving unsigned electronic documents or entries, the organization requires a process to identify qualified alternate signers for purposes of record closure. A qualified alternate signer is one who is able to uphold the purpose of attestation, is familiar with the clinical case, and can validate the accuracy of the documentation.

When entries must be left unsigned due to unfamiliarity by other caregivers and a lack of alternate signers, explanatory documentation should be included in the EHR to indicate the reason for record closure with e-signature validation gaps. Organizations should develop clear policies and procedures or medical staff bylaws on how to authenticate unsigned documents. The e-signature statement should indicate who signed and who the alternate signer signed for.

Proxy signatures (alternate or group signatures). Organizations also require processes by which a provider is authorized to electronically sign documentation on behalf of the original author. The proxy accepts responsibility for the content of the original documentation. Organizational policy should outline monitoring practices to detect inappropriate electronic proxy signature practices, whether from ignorance, negligence, or overt policy abuse.

Auto-attestation (also known as auto-authentication). Auto-attestation is the process by which an entry is implicitly signed (attested) through the user authentication process at sign-on. It is also the process by which a physician or other practitioner

attests an entry that he or she cannot or has not reviewed because it has not yet been transcribed or the electronic entry cannot be displayed.

Healthcare organizations must consult legal counsel if they choose to pursue this approach. Federal regulations (both the Uniform Electronic Transactions Act and Medicare Conditions of Participation for Hospitals) require each author take a specific action to verify and attest an entry. In general, auto-attestation is not a recommended practice.

Batch signing. Batch signing is the process of applying a signature to multiple entries at one time. Batch signing of entries or physician orders may be acceptable if the following criteria can be met:

- All entries or orders can be viewed.
- Each entry or order can be acted upon individually, including editing the content.
- The entry or order can be removed from the batch.

Scribes. Some providers use scribes or assistants to type entries into the system for subsequent authorization. Organizations must put checks and balances in place to ensure that the physician or other legally responsible individual has reviewed the health record entries and authenticated them.[4] Organizations assign scribes unique user IDs to identify them as the authors of the entries and require the authorized providers or physicians to attest to the accuracy of the entries.

Data Elements for Display of E-Signatures

The full printed name of the author should appear at the end of an entry or document with the date and time, the digitized signature, or a signature statement with the author's credentials. For example, "Electronically signed by Dr. John Doe on 6/1/09 at 01:15am" or an abbreviation such as "/es/Dr. John Doe, 6/1/09; 01:15am."

The following are examples of statements that should be readable and viewable as part of the electronic record, output, or printed report. The statements may vary across healthcare entities, but should be based on the intent of the signature:

- Electronically signed by
- Signed by
- Authenticated by
- Sealed by
- Data entered by
- Approved by
- Completed by
- Verified by
- Finalized by
- Validated by
- Generated by
- Confirmed by
- Reviewed by

In the event of an addendum to a transcribed record, the addendum should be added to the top or bottom of the report and a second e-signature applied that includes the date and time the addendum was electronically signed. For example:

- Electronically signed by John Doe, M.D. on 6/1/09 at 01:15am
- Electronically signed by John Doe, M.D. on 6/2/09 at 03:45pm

When more than one signature is required, such as in the case of a resident or physician assistant dictating under the supervision of a physician, both signatures should appear on the bottom of the report similar to the sample format above.

For those systems that do not support dual signature functionality, an alternative is to have a statement on the bottom of the report that reads "Dictated by Mary Smith, PA, under the supervision of Dr. John Smith," with the electronic signature affixed by the supervising physician. The process for handling multiple signatures should be addressed in organizational policy.

If initials are displayed on a screen or printed view of a document, such as on a flowsheet, the full signature should be referenced on the document.

Additional guidance on signatures related to billing for residents, certified nurse practitioners, and the attending can be found in the AHIMA practice brief "Applying the Teaching Physician Guidelines." [*J AHIMA*, August 2009]

Preliminary (Pending) Entries and Documents

A preliminary entry is documentation that is available for viewing but has not been authenticated or attested. This is not to be confused with an incomplete entry or documentation, where an entry or dictation is started but never completed.

Some systems may not allow preliminary entries and may require a signature in order for the document to be displayed in the EHR. In these cases, versioning should be used. This guidance applies to entries in the EHR as well as transcribed documents. Where applicable, these entries and documents should display a header or watermark stating the document has not yet been authenticated, such as "Draft Copy," "Pending," "Preliminary," or similar language. Organizations will need to determine the viewing ability of unsigned documents.

Organizations should also develop a policy outlining the process to clean up unsigned documents. Without such a policy, documents could remain in the system for long periods of time, hindering patient care. A regular process for monitoring pending notes also should be implemented.

Amendments, Corrections, Retractions, and Deletions in the EHR

Handling amendments, corrections, retractions, and deletions in the EHR is complex and varies based on the system. The process flow diagram illustrates the proper way to handle changes to EHR records. The signature event closes the record, and any subsequent changes are handled as a new version. All versions are retained.

Organizations must evaluate the proper handling of these situations in all clinical applications that are part of the EHR. Along with proper system functionality, organizational policies should address handling of each change.

The AHIMA toolkits "Amendments, Corrections, and Deletions in the Electronic Health Record Toolkit" and "Amendments, Corrections, and Deletions in Transcribed Reports Toolkit" assist with proper implementation of these complex issues.

Version Management and Retention

If policy allows signed documents to be edited, all signed versions must be available for medico-legal purposes. There must be a procedure for accessing each version. If documents in the e-signature application are the legal medical record copy, no signed documents can be deleted permanently from the system. If documents are printed and maintained as part of a hard-copy record or are transferred to another system or repository, this is not an issue.

If a document or note is available for use before it is finalized and signed, a version of the unsigned record must be retained for medico-legal purposes if changes were made.

E-Signature Lifecycle

When evaluating EHR systems and electronic document management systems it is important to determine whether the e-signature functionality is part of the electronic system or another piece of software attached to the system for authentication purposes. In either case the signature must be retained the same length of time as the record to which it is appended.

As the custodians of the record, HIM professionals bear the responsibility of ensuring that the EHR and the electronic document management system maintain the signature tied to the content for the required length of time. This applies to all clinical applications that are sources for the legal health record.

Security of Passwords and PINs

Secure e-signature methods have become more readily available over the last decade as technology has advanced. However, many facilities have been hesitant to implement these options for fear of disrupting clinicians' preferred workflow. The recommended best practice for e-signatures is authentication and a second level of identification to attest to authorship either through use of a PIN, biometric scan, secure ID card, or digital signature.

Passwords or other personal identifiers must be controlled carefully to ensure that only the authorized individual can access the EHR system and apply a specific e-signature. Each individual who accesses the EHR and signs records must have his or her own identifier. Use of an administrative log-in or shared log-in will contaminate the integrity of the legal health record. If the system allows administrative sign-on, there is no guarantee that the correct author has signed the entry, thus compromising the integrity of the record and creating legal concerns.

Since the e-signature password is tied to the system log-on process, unencoded passwords should not be sent across networks. For organizations that use passwords, the following password or PIN characteristics are recommended to strengthen password security and simplify password management for the end user:

- Passwords should be a minimum of six to eight characters.
- Characters should be case sensitive and contain at least one alpha and one numeric character and special characters.
- Users should be unable to reuse passwords for at least three password change cycles.
- Users should be able to change their own passwords or PINs for increased flexibility and control.
- Passwords should be set to automatically expire after a set elapsed time with user prompts to set new password at next log-on.
- Organizations should prohibit group or shared passwords, overuse of administrative passwords, or group passwords. Attestation, access controls, audit records, and other security features are all dependent on the accurate identification and authorization of the user; use of group and shared passwords will cause catastrophic failure of security protocols and render the legal health record useless.

Finally, practitioners authorized to use e-signatures should be required to sign a statement acknowledging their responsibility and accountability for the use of their e–signature stating that they are the only one who has access to and will use their specific signature code. Organizational policy should define appropriate disciplinary actions for inappropriate use or sharing of unique identifiers.

HIM Operations

Allowing clinician access to the EHR does not come without challenges. Every electronic signature location—nursing unit, HIM department, personal office, or home—has to be carefully considered to ensure patient health information is protected. Therefore, deciding which clinicians will be able to electronically sign charts, as well as what, where, and how they may sign, is imperative.

Determining who will support the system is equally important. Organizations will need to provide ongoing support. To minimize confusion, clinicians should be given one number to call for assistance; if possible, an existing help desk system in the facility.

Staff familiar with the application can provide a backup to the help desk staff when needed. Super users or staff familiar with the application in the HIM department or other departments can support staff changes over time.

The application should be available at all times. However, organizations will need to analyze whether access issues of availability are different on and off site. Policies need to address availability while backups are performed or system updates or upgrades are installed. If the network has routine or extended downtimes, procedures for notifying users must be clear. In addition, organizations must negotiate support agreements that support around-the-clock access.

It is important that policies address the need to monitor or review all documents and documentation to ensure e-signatures are affixed and recorded in a timely manner. Periodic audits are recommended to confirm display of e-signatures and that interfaces between systems work as intended.

HIM departments should maintain a list of physicians or other healthcare practitioners who are authorized to use e-signatures. Organizations in the midst of migrating to a full EHR require a way to distinguish among documents to be manually signed and those that are electronically signed.

It is important for HIM professionals to identify what information is available from the application and evaluate its usefulness as a monitoring tool to ascertain whether a user viewed, edited, or printed any documents or pages. Policy and procedures should include assigning responsibility for evaluating exception reports, audit trails, and other access reports.

Finally, it is best to confirm the application has a method to ensure content completion and the validity of a signature by allowing the author to individually review and attest each entry one at a time.

Staff will require written procedures to follow if the application is unavailable. It is recommended that staff wait for restoration of the application rather than revert to manual signatures. A decision to revert to paper must not be made lightly. It is nearly impossible for HIM staff to reconcile documents that were signed manually with those waiting for electronic signature while the application was unavailable. Any difference in procedures depending on the duration of the downtime, or if the downtime is planned or unplanned, should be clear.

Organizational policy must address system access and monitoring, handling of authorship issues and data elements, changes to records, security and handling of passwords, support, and disciplinary action.

Documents signed electronically must be retained in conformity with the organization's definition of the legal health record and retention policy.

E-signatures are complex by nature, yet they are critically important to support the organization's legal health record. Proper attention to system functionality, regulatory requirements, and organizational policies is required for successful implementation and ongoing management.

Appendixes

Appendix A: HL7 EHR-System Records Management and Evidentiary Support Functional Profile Standard Excerpt
Appendix B: Laws, Regulations, and E-Signature Acts
Appendix C: E-Signature Model Policy Considerations
Appendix D: Glossary of Terms
Appendix E: Amendments, Corrections, and Deletions in Transcribed Reports Toolkit

Notes

1. Health Level Seven. HL7 EHR System Records Management and Evidentiary Support Functional Profile 2009. Available online at www.hl7.org.
2. Smedinghoff, Thomas, and Ruth Hill Bro. "Electronic Signature Legislation." FindLaw Library. January 1999. Available online at http://library.findlaw.com/1999/Jan/1/241481.html.
3. Joint Commission. *2009 Comprehensive Accreditation Manual for Hospitals (CAMH): The Official Handbook*. Oak Brook, IL: Joint Commission Resources, 2008.
4. AHIMA. "Guidelines for EHR Documentation to Prevent Fraud." *Journal of AHIMA* 78, no. 1 (Jan. 2007): 65–68.

Resources

AHIMA. "Update: Maintaining a Legally Sound Health Record—Paper and Electronic." *Journal of AHIMA* 76, no. 10 (Nov/Dec 2005): 64A–L.

American Bar Association. "Digital Signature Guidelines." Available online at www.abanet.org/scitech/ec/isc/dsgfree.html.

ASTM International. ASTM E1762-95(2003) Standard Guide for Electronic Authentication of Health Care Information. Available online at www.astm.org/Standards/E1762.htm.

Certification Commission for Healthcare Information Technology. "Criteria and Test Scripts." 2009 Final Ambulatory EHR Criteria and Test Scripts plus Child Health and Cardiovascular Medicine Options. Available online at www.cchit.org/participate/cts.

Colorado Secretary of State. Uniform Electronic Transactions Act (UETA) Program. Available online at www.sos.state.co.us/pubs/UETA/UETA_Home_Page.htm.

E-HIM Work Group on Implementing Electronic Signatures. "Implementing Electronic Signatures." October 2003. Available online in the AHIMA Body of Knowledge at www.ahima.org.

Federal Information Processing Standards Publication 186. May 19, 1994. Available online at www.itl.nist.gov/fipspubs/fip186.htm.

International Law and Policy Forum. "An Analysis of International Electronic and Digital Signature Implementation Initiatives." September 2000. Available online at www.ilpf.org/groups/analysis_IEDSII.htm.

International Organization for Standardization. ISO/IEC 14888-3 Information Technology–Security Techniques–Digital Signatures with Appendix. Available online at www.iso.org.

International Telecommunication Union. Available online at www.itu.int/en/pages/default.aspx.

IsSolutions, LLC. Available online at www.goissolutions.com.

Nunn, Sandra. "Enterprise E-Signature: Managing Flourishing E-Signatures at the Organizational Level." *Journal of AHIMA* 80, no. 5 (May 2009): 48–49.

Prepared By

Donna Barron, BA, RHIT
Lauren Blumenthal, RHIA, PMP
Suzonne Bourque, RHIA, CCS
Natasha Brovarny, RHIT
Jennifer Childress, RHIT
Jill S. Clark, MBA, RHIA
Dawn L. Criswell, MS, RHIA, FAHIMA
Julie Dillard, MHA, RHIA
Michelle Dougherty, MA, RHIA, CHP
Marie Gardenier, MBA, RHIA, CHPS
Darice Gryzbowski, MA, RHIA, FAHIMA
Terri Hall, MHA, RHIT, CPC, CAC
Marla Hardison, CCS-P
Janice Hecht, MBA, RHIA
Beth Hjort, RHIA, CHPS
Kim Jackson, RHIT, CHP
Mary Johnson, RHIT, CCS-P
Diane M. Lerch, RHIA, CHPS, CCS, CHA
Dorothy W. Maxim, MS, RHIA
David Ike Mozie, PhD, RHIA
Indra Osi, RHIA, CHP
Deanna Panzarella
Janis L. Pavlick, RHIA
Ulkar Qazen, MSJ, RHIA
Sharron Ray, MHA, RHIA, MT, ASCP
Linda Spurrell, LPN, RHIT, CHP
Dolores Stephens, MS, RHIT
Susan Sugg, MSA, RHIA, PMP
Vicky Turner-Howe, RHIT, CCS
Kim Vernon, RHIA

Traci E. Waugh, RHIA
Lou Ann Wiedemann, MS, RHIA, CPEHR

Acknowledgments

Beth Acker, RHIA
Rhonda L. Anderson, RHIA
Mark S. Dietz, RHIA
Angela K. Dinh, MHA, RHIA
Sheila Green-Shook, MHA, RHIA, CHP
Tracy G. Hickey, MBA, RHIA
Deborah Kohn, MPH, RHIA, CHE, FACHE, CPHIMS, FHIMSS
Kelly McLendon, RHIA
Mary Meysenburg, MPA, RHIA, CCS
Debra Musa-Cross, RHIT, CHP
Kimberly Baldwin-Stried Reich, MBA, MJ, RHIA, CHC, CPHQ
Heather Black Shea, JD
Monica Tormey, RHIA

The information contained in this practice brief reflects the consensus opinion of the the professionals who developed it. It has not been validated through scientific research.

Article citation:
AHIMA e-HIM Work Group: Best Practices for Electronic Signature and Attestation. "Electronic Signature, Attestation, and Authorship (2009 update) - Retired" *Journal of AHIMA* 80, no.11 (November 2009): [expanded online version].
