# Electronic Signatures (1998) - Retired

Save to myBoK

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

---

*Note: The likeness of a patient may be recorded through a number of visual means, including still photography, videotaping, digital imaging, scans, and others. Throughout this document, the term "patient photography" will be used for any such recording of a patient's likeness.*

## Background

In computer-based patient records, an electronic "original" is created on a computer screen. Responsible healthcare practitioners authenticate, or sign, entries in the record in several different ways, most commonly by entering a unique code or password that verifies the identity of the healthcare practitioner and creates an individual "signature" on the record. Usually this signature is represented by a statement such as "Electronically signed by John Smith, MD (date/time)." The record is then stored on magnetic, optical, or other computer storage media.

Digital identification capabilities are used for complete verification of electronic documents. Public key cryptography uses a matched pair of public and private keys. One key is used to encrypt the document, and only the corresponding key can decrypt it. A digital ID has four basic components: a public key that corresponds to a person, a private key, the name and identification of the person, and a digital signature from a trusted digital ID issuer. An application puts a person's *digital signature* on a document by calculating the document's unique "thumbprint," using a cryptographic equation. The thumbprint is then encrypted for privacy using the person's private key and stamped on the document. A recipient can later decrypt the digital signature (using the person's public key) and match the original thumbprint of the document with the thumbprint calculated by the recipient's application. A match indicates two things: that the document was generated by the person who is supposed to have sent it and that it has not been altered.

A digital signature is not the same as a *digitized signature*. A digitized signature is generated by converting an actual written signature to an electronic image. The digitized signature uses a handwriting recognition algorithm, and there have been problems with the reliability of these algorithms. A digitized signature looks much the same as the original, but it does not provide the same protection as a digital signature. A digitized signature can be forged easily, and a forgery is more difficult to detect.

Digitized signatures also may be copied and applied to other documents. With a digitized signature, there is no way to tell if a document has been altered after it left the signer.

(It should be noted that electronic signature systems are not the same as auto-authentication or auto-signature systems, some of which do not allow the healthcare practitioner to review the entry before signature and some of which do not require specific action by the healthcare practitioner to authenticate an entry.)

## Accreditation Requirements

The use of electronic signatures is acceptable to the Joint Commission on Accreditation of Healthcare Organizations. According to the 1998 *Comprehensive Accreditation Manual for Hospitals (CAMH)*, Standard IM.7.8, "entries may be confirmed by written signatures or initials, by rubber-stamp, or computer 'signatures' (or sequence of keys)." In the CAMH, the Joint Commission outlines specific requirements for the use of rubber-stamp and electronic signatures:

- The practitioner must sign a statement that he or she alone will use it
- A stamp or electronic signature authorized for one person is not used for anyone else

The Joint Commission also requires that the computer system allow the author to review the document online before signing it electronically. The Joint Commission accepts the use of electronic signatures in other care settings too. The use of electronic signatures is noted to be acceptable in ambulatory care, home care, long term care, and mental health, subject to the requirements outlined above.

## Legal and Regulatory Requirements

To participate in the Medicare program, healthcare organizations must comply with federal regulations promulgated by the Health Care Financing Administration (HCFA), which are commonly referred to as the Medicare Conditions of Participation. The use of electronic signatures is acceptable under the Medicare Conditions of Participation. 42 Code of Federal Regulations, Section 482.24, Conditions of Participation for Hospitals, Condition of Participation: Medical Record Services (c)(1)(iii) states, "Authentication may include signatures, written initials, or computer entry." According to HCFA's "Hospitals Interpretive Guidelines and Survey Procedures," a list of computer codes and written signatures must be readily available and maintained under appropriate safeguards. Sanctions must be established for improper or unauthorized use of rubber-stamp and electronic signatures. In addition, the use of electronic signatures must be authorized by the organization's governing body.

Medicare Conditions of Partici-pation for other care settings have requirements that entries be signed, but acceptable methods of authentication are not specified. Require-ments for States and Long Term Care Facilities (42 CFR Ch. IV, Part 483, Subpart A, Section 483.40) requires that physicians "write, sign, and date progress notes at each visit and sign and date all orders." Conditions of Participation for Hospice Care (42 CFR Ch. IV, Subpart C, Section 418.74) requires that "entries are made and signed by the person providing the services." Conditions of Participation for Home Health Agencies (42 CFR, Ch. IV, Section 484.48) requires "signed and dated clinical and progress notes." Conditions of Participation for Rural Primary Care Hospitals (42 CFR Ch. IV, Section 485.638) requires "dated signatures of the doctor of medicine or osteopathy or other health care professional."

Medicare Conditions of Partici-pation for Comprehensive Outpatient Rehabilitation Facilities (42 CFR Ch. IV, part 485) and Ambulatory Care Surgical Services (42 CFR Ch. IV, part 416) do not address signature requirements for patient record entries.

Public Law 104-191, the Health Insurance Portability and Account-ability Act (HIPAA), mandates that the Secretary of Health and Human Services, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures. The notice of proposed rule making that pertains to electronic signature was published in August 1998.

State laws and regulations on authentication of medical records vary widely. Some are silent on authentication of medical records, while others simply require medical records to be maintained according to recognized professional standards. On the other hand, some states are very specific as to how practitioners must authenticate medical record entries, outlining requirements for the use of electronic signatures. States with specific laws or regulations addressing electronic signatures are listed in Exhibit 1.

If your state has not authorized authentication of medical record entries by electronic signature -- either by statute or regulation -- check with your state licensing authority to see if it permits the use of electronic signature. Some states, including Florida, New Hampshire, and Texas, do not address this issue in their statutes or regulations but do permit the use of electronic signature with approval from fiscal intermediaries or state authorities.

## ASTM Standard

The American Society for Testing and Materials (ASTM) has developed guidelines for the use of electronic signatures based on the principles of accountability, data integrity, and nonrepudiation (once applied, the signature could not be disavowed by the signer).

ASTM Subcommittee E31.20 on Authentication of Computer-based Health Information, part of Committee E31 on Computerized Systems, developed the Standard Guide for Electronic Authentication of Health Care Information. The standard addresses:

- nonrepudiation
- integrity
- secure user authentication
- multiple signatures
- signature attributes
- countersignatures
- transportability
- interoperability
- independent verifiability
- continuity of signature capability

To obtain a copy of this standard guide, call ASTM's Customer Service Department at (610) 832-9500. Ask for standard guide #E1762-95. There is a small charge, with different fees for ASTM members and nonmembers.

## Security Issues

To assure the accuracy and protect the integrity of computer-based patient records, AHIMA recommends the following safeguards:

1. Healthcare practitioners should be given an opportunity to review their entries for completeness and accuracy prior to electronically signing them.

2. Once an entry has been signed electronically, the computer system must prevent it from being deleted or altered. If the signed entry is converted to another format (for example, between various image formats), the electronic signature applies only to the original format. If errors are later found in the entry or if information must be added, this should be done by means of an addendum to the original entry. The addendum should also be signed electronically and date/time stamped.

3. Passwords or other personal identifiers must be controlled carefully to assure that only the authorized individual can apply a specific electronic signature. Any practitioner authorized to use electronic signatures should be required to sign a statement that he/she is the only one who has access to and will use his/her specific signature code. Since the electronic signature password is tied to the system log-on routine, unencoded passwords should not be sent over networks.

4. An organization's medical staff or its medical record committee should approve the use of electronic signature and develop rules and regulations governing its use. These rules and regulations should contain appropriate sanctions for misuse and should clearly prohibit individuals from delegating their electronic signature authorization to another person.

5. The healthcare organization and affected departments should adopt and enforce policies and procedures to safeguard against unauthorized use of electronic signatures.

6. The health information management department should maintain a list of physicians or other healthcare practitioners who are authorized to use electronic signatures.

7. The organization's administrative offices should maintain a list of the practitioners' computer codes under appropriate safeguards.

8. Healthcare facilities with integrated information systems should support a single electronic signature capability to enable users to sign entries supported by different systems without using multiple passwords.

## References

Bearden, Mary. "Legal Update: Electronic Signatures on Medical Records." *Journal of the Texas Health Information Management Association* Jan./Feb./March 1992.

Endrijonas, Janet. *Data Security.* Rocklin, CA: Prima Publishing, 1995.

Goldsborough, Reid. "Signing Documents in the Electronic Age: A Look at Privacy, Legal Issues." *PC Today* December 1995: 79-81.

Health Care Financing Administration. *Medicare/Medicaid State Operations Manual.* Appendix A. "Hospitals Interpretive Guidelines and Survey Procedures." Springfield, VA: US Department of Commerce, 1986.

Joint Commission on Accreditation of Healthcare Organizations. *1998 Comprehensive Accreditation Manual for Hospitals.* Oakbrook Terrace, IL, 1998.

Joint Commission on Accreditation of Healthcare Organizations. *1998 Accreditation Manual for Ambulatory Care.* Oakbrook Terrace, IL, 1998.

Joint Commission on Accreditation of Healthcare Organizations. *1998 Accreditation Manual for Home Care*. Oakbrook Terrace, IL, 1998.

Joint Commission on Accreditation of Healthcare Organizations. *1998 Accreditation Manual for Long Term Care.* Oakbrook Terrace, IL, 1998.

Joint Commission on Accreditation of Healthcare Organizations. *1998 Accreditation Manual for Mental Health, Chemical Dependency, and Mental Retardation/Developmental Disabilities Services.* Oakbrook Terrace, IL, 1998.

Medicare Conditions of Participation for Home Health Agencies, 42 CFR Ch. IV, Section 484.48.

Medicare Conditions of Participation for Hospice Care, 42 CFR Ch. IV, Subpart C, Section 418.74.

Medicare Conditions of Participation for Rural Primary Care Hospitals, 42 CFR Ch. IV, Section 485.638.

Medicare Conditions of Participation for States and Long Term Care Facilities, 42 CFR Ch. IV, Part 483, Subpart A, Section 483.40.

Roach, William H., Jr., et al. *Medical Records and the Law.* Gaithersburg, MD: Aspen Publishers, Inc., 1994.

"The New Standard Guide for Electronic Signatures." *ASTM Standardization News* August 1995: 14-17.

Tomes, Jonathan P. *Compliance Guide to Electronic Health Records: A Practical Reference to Legislation, Codes, Regulations, and Industry Standards.* New York: Faulkner & Gray, 1998.

## Prepared by

Harry Rhodes, MBA, RRA, HIM practice manager

*Note: This practice brief replaces an earlier practice brief published in the March 1996* Journal of AHIMA.

## Acknowledgments

Assistance from the following individuals is gratefully acknowledged:

AHIMA's Component State Associations
Donna Fletcher, MPA, RRA
Kathleen Frawley, JD, MS, RRA

**Recommendations**

- Before applying an electronic signature, healthcare practitioners should have an opportunity to review their entries for completeness and accuracy -- correcting or modifying them as needed.
- Once an entry has been signed electronically, the computer system must prevent it from being deleted or altered. If errors are found later in the entry or if information must be added, this should be done by means of an addendum to the original entry. Both the original entry and the addendum should be date/time stamped by the computer at the time the entry is signed electronically.
- Passwords or other personal identifiers must be controlled carefully to assure that only the authorized individual can apply a specific electronic signature.
- An organization's medical staff or its medical record committee should approve the use of electronic signature and develop rules and regulations governing its use.
- To comply with Medicare Conditions of Participation, governing body approval of electronic signature also should be obtained.
- The health information management department should maintain a list of physicians or other healthcare practitioners who are authorized to use electronic signatures.
- The organization's administration should maintain a list of the practitioners' computer codes under appropriate safeguards.
- Any practitioner authorized to use electronic signatures should be required to sign a statement that he or she is the only one who has access to and will use his or her specific signature code.

| State | Summary of Law/Regulation | Cite |
|---|---|---|
| Alaska | Authentication by computer key instead of a physician's signature is permitted when the physician has given a signed statement to the hospital administration that he or she is the only person who has possession of the stamp or key and who may use the stamp or key. | Alaska Admin.Code, 7 AAC 12.770(e) |
| Arkansas | Electronic or computer-generated signatures are acceptable as authentication if the signature is generated by a confidential code that only the user possesses. Safeguards outlined for the use of rubber stamps should be followed for the use of electronic signatures. | Arkansas Dept. of Health, Rules and Regs. for Hospitals and Related Institutions in Arkansas. Arkansas Reg. 0601 H |
| California | Physicians, dentists, or podiatrists may authenticate medical records with a signature stamp or computer key in lieu of a physician's signature only when that physician hasplaced a signed statement in the hospital administrative offices to the effect that he or she is the only person who has possession of the stamp or key and will use the stampor key. Similar requirements are outlined for other types of healthcare facilities. | 22 California Code Regs. tit. 22, Section 70751 (g)(1)(2) (hospitals), Section 71551 (g) (1)(2) (acute psychiatric hospitals), Section 79351 (g) (1)(2) (chemical dependency |

| | | |
|---|---|---|
| | Note: Facilities planning to implement electronic signature systems are advised tocontact the California Department of Health Services, Licensing and Certification Division for additional requirements for electronic signature systems. | recovery hospitals), California Health & Safety Code Section 1795.28 (additional requirements for electronic record keeping systems) |
| Colorado | Hospital licensing standards issued by the state department of health permit authentication by "written signature, identifiable initials, or computer key." Rubber-stamp signatures are permissible if the individual places a signed statement in the hospital administrative offices stating that he or she is the only person who has possession of the stamp and is the only person who will use it. | Colorado Dept. of Health, Licensing Standards for General Hospitals, Section 4, Medical Records, Para. 4.4 |
| Connecticut | Electronic signatures are permitted for medical records. Rules and regulations for their use are in development. In the meantime, hospitals should submit any current or proposed protocol for the use of electronic signatures for medical records-including protections for patient confidentiality and medical record security-to the Department of Public Health and Addiction Services for review and approval. | Connecticut Public Act 93-317 |
| Delaware | Delaware follows the federal requirements for medical records except for nursing homes. Thus, the Medicare Conditions of Participation, which permit electronic signatures, appear to allow Delaware providers to use electronic signature. The Nursing Home Regulations for Skilled Care, however, do not address authentication. | |
| District of Columbia | Hospital medical records must follow the requirements of the Joint Commission, as set forth in the Standards for Hospital Accreditation. | District of Columbia Mun. Regs. tit. 22 Section 2216.4 |
| Hawaii | Hawaii law specifies that medical records may be computerized (or reduced by the use of microfilm or other similar photographic process), provided that the method used creates an unalterable record. Thus, the use of electronic signature appears to be | Hawaii Rev. Stat. Section 622-58 permissible. |
| Illinois | Written signatures or initials and electronic signatures or computer-generated signature codes are acceptable as authentication. All signatures or initials, whether written, electronic, or computer-generated, must include the initials of the signer's credentials. For a hospital to employ electronic signatures or computer-generated signature codes for authentication purposes, the hospital's medical staff and board must adopt a policy that permits authentication by electronic or computer-generated signature. The policy mustidentify those categories of the medical staff, allied health staff, or other personnel within the hospital who are authorized to authenticate patient records using electronic or computer-generated signatures. The policy must include at least the following safeguards: (1) each user must be assigned a unique identifier that is generated through a confidential access code; (2) the hospital must certify in writing that each identifier is kept strictly confidential, and use of an identifier will be terminated if it is misused; (3) the user must certify in writing that he or she is the only person authorized to use the signature code; and (4) the hospital must monitor the use of identifiers and take corrective action as needed. To ensure that the content of authenticated entries is accurate, there must be a verification process that includes the following:<br>• certain designated fields for each type of document must be completed before it may be authenticated, with no blanks, gaps, or obvious contradictory statements appearing in those fields<br>• correction or supplementation of previously authenticated entries must be made by additional entries, which are separately authenticated | Illinois Hospital Licensing Act and Hospital Licensing Requirements, 77 Illinois Admin. Code 250, Chapter I Section 250.1510, Subchapter b, Subpart L(c) |

| | | |
|---|---|---|
| | • the user must have an opportunity to verify that the document is accurate and that the signature has been properly recorded<br>• the hospital must periodically sample records generated by the system to verify the accuracy and integrity of the system Each report generated by a user must be separately authenticated. | |
| Indiana | Physician's orders for medication and other specified services must be in writing or acceptable computerized form, and the attending physician must sign them by hand or key within 24 hours. All entries in medical records must be dated and authenticated, and the facility must establish a method to identify the authors of entries. Such identification may include signatures, initials, or computer keys. Note: The Board of Health supports the use of electronic signatures only if certain criteria are met, including a requirement that the author has the ability to review the document prior to signing it. | Indiana Admin. Code tit. 410, r. 15-1-9(d) |
| Louisiana | A Louisiana statute authorizes electronic signatures by licensed healthcare providers. The Department of Health promulgates rules for their use. | 40 Louisiana Rev. Stat. Ann. Section 2144 |
| Mississippi | Authentication may include signatures, written initials, or computer entry. A list of computer codes and written signatures must be readily available and maintained under adequate safeguards. There shall be sanctions established for improper or unauthorized use of stamp and computer key signatures. | Mississippi State Board of Health, Hospital Licensing Regs., Chap. 17, Medical Records, Para. 1709, Amended 1993 |
| Missouri | Acceptable methods of authentication include written signatures, initials, computer-generated signature codes, or rubber-stamp signatures. | 6 Missouri Code Regs. tit. 13, Section 50-20.020(3)(D) |
| Nebraska | Physicians must sign and date all orders in ink or indelible pencil or enter them into a computer using a physician code system. Subject to individual hospital policies, they may use facsimiles or codes for physician signatures and initials where appropriate safeguards limit access and use of the facsimile or code. | Nebraska Dept. of Health, Rule 30, Regs. and Standards for Hospitals (3)(d)i. Nebraska Admin. Rules and Regs. 175-9- 003.04A2 |
| Nevada | Allows healthcare records to be created, authenticated, and stored in a computer system that limits access to those records. | Nevada Rev. Stat. Ann. Section 629.051 |
| New Jersey | All entries must be written in ink, dated, and either signed by the recording person or authenticated through the use of a computerized medical record system. | New Jersey Admin. Code, tit. 8, Section 43G- 15.2(b)(1993) |
| New York | Upon completion of ordering, providing, or evaluating patient care services, the provider must record and promptly enter such actions into the patient medical record, legibly and completely. The person making the entry must authenticate it with a signature, written initials, or computer entry. | New York Comp. Rules and Regs. tit. 405 Section 505.11(b) |
| North Carolina | All orders for medication or treatment must be authenticated at the time of recordation by the ordering physician. Verbal orders must be authenticated within 24 hours after they are given by the ordering physician or by a physician involved in the care of the patient. Authentication must be accomplished by signature, initials, computer entry or code, or other method(s) not inconsistent with the laws, rules and regulations, or any other applicable jurisdictions. | North Carolina Admin. Code, tit. 10, Section 03C.0405 |
| North Dakota | If appropriate safeguards have been taken to limit access to medical records in an electronic data storage system, a medical record in an electronic storage system may be authenticated by an electronic signature or a computer-generated signature code. | North Dakota Century Code Section 31-08-01.2 |
| Ohio | Any entry into a healthcare record may be authenticated by executing handwritten signatures or handwritten initials directly on the entry or by executing an electronic signature. An electronic signature executed in accordance with an electronic signature system that is certified by the department of health under | Ohio Admin. Code Section 3701.75 (3) (B) |

| | | |
|---|---|---|
| | division (C) of this section shall be considered for all legal purposes to be the same as having executed a hand- written signature or handwritten initials, except when any federal law governing state participation in a federal program requires that entries into healthcare records be authenticated only by handwritten signatures or handwritten initials. | |
| Oklahoma | Electronic or computer-generated signatures of a physician are acceptable as authentication and may be used in any place in the medical record where a physician's signature is required, including, but not limited to, all medical orders. The signature must be generated by a confidential code, which only the user possesses. The physician must have a signed statement on file in the hospital administrative offices that states the physician will use electronic signatures to authenticate his or her entries in the medical record, that the signature will be generated by a confidential code which only the physician possesses, and that no other person will be permitted to use the signature. The physician's use of electronic signature must be approved in writing by the hospital's administrator and medical records committee. The electronic signature must be the full legal name of the physician, including the physician's professional title. The State Board of Health is authorized to promulgate rules and regulations pertaining to electronic signatures. | Oklahoma Stat. tit. 63, Section 1-722 |
| Oregon | Orders of a physician, dentist, podiatrist, or other individual authorized within the scope of his or her professional license and within hospital privileges must be dated and signed by such person or authenticated by a signature stamp or computer key. Authentication may be done by stamp or computer key only when the person has placed a signed statement in the hospital administrative offices to the effect that he or she is the only person who has possession of the stamp or key and who will use the stamp or key. All entries in patients' medical records must be dated, timed, and authenticated. Verification of an entry requires use of a unique identifier, such as signature, code, thumbprint, voice print, or other means that allows for identification of the individual responsible for the entry. | Oregon Admin. R.333-505-050(3)(h) |
| Pennsylvania | All entries in medical records must be dated and authenticated. Pennsylvania defines "to authenticate" as "to verify authorship, for example, by written signature, identifiable initials, or computer key." Specific requirements are outlined for the use of rubber- stamp signatures. | 28 Pennsylvania Code 7.2, Section 101.4 |
| Rhode Island | Where any rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by an electronic signature. | Rhode Island Electronic Signatures and Records Act, Section 42-127-1 through Section 42-127-5 |
| South Dakota | A healthcare facility must ensure that entries to the medical record are signed or electronically authenticated. If the facility permits any portion of the medical record to be generated by electronic or optical means, policies and procedures must exist to effectively limit the use of authentication by unauthorized users. | South Dakota Admin.Rules, Section 44:04:09:07 |
| Tennessee | The requirements for signature or countersignature by a physician, dentist, podiatrist, or other person responsible for signing, countersigning, or authenticating an entry may be satisfied by the electronic entry by such person of a unique code assigned exclusively to him or her, or by entry of other unique electronic or mechanical symbols, provided the person has adopted this as his or her signature in accordance with established hospital protocol or rules. | Tennessee Dept. of Health, Board for Licensing Health Care Facilities, Chapter 1200-8, Hospital Rules and Regs. Ch. 1200-8-3-.02(7) |
| Utah | The author of any entry in a medical record compiled or maintained by a healthcare facility may authenticate it with a signature, including first initial, last name, and discipline, or use of a computer identification process unique to the author that definitively identifies the author. | Utah Code Ann. Section 26-21-21 |
| Washington | The person who gave the order, provided the care, or performed the observation, assessment, treatment, or other service must date and authenticate each entry in | Washington Admin. Code Section 248-318-440 |

| | | |
|---|---|---|
| | a patient's medical record. Entries must be legibly written in ink, typewritten, or recorded on a computer terminal designed to receive such information. | |
| West Virginia | The West Virginia Medical Practice Act authorizes medical service professionals to use an "electronic signature or unique electronic identification to effectively sign materials, transmitted by computer or other electronic means, upon which [a] signature is required for purposes related to the provision of medical services." | West Virginia Code, Section 30-3-13 |

**Issued: October 1998**

---