Electronic Signature, Attestation, and Authorship. Appendix B: Laws, Regulations, and Electronic Signature Acts (2013 update)

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 with the system that authorizes the individual to access the system (e.g., the sign-on process). Authenticating is important because it assigns responsibility for an entry they create, modify, or view. **Attestation**, on the other hand, is the act of applying an electronic signature to the content, showing authorship and legal responsibility for a particular unit of information.

Therefore, HIM professionals should keep in mind the use of these terms and their evolution when reviewing the laws, regulations, and electronic signature acts listed below. The laws, regulations, and acts listed below can help HIM professionals in developing and implementing e-signature functionality and policy in their organizations.

Uniform Electronic Transactions Act

The Uniform Electronic Transaction Act (UETA) equates electronic signatures to manual signatures. It requires that the signer execute or adopt a sound, symbol, or process with the intent to sign the record. Additionally, UETA requires that the electronic signature be linked or logically associated with the electronic record being signed.

UETA makes clear that anything electronic would suffice, including voice recordings, Web browser clicks, and other symbols or keystrokes to indicate intent. Under UETA, any type of digital information could be considered to be either a signature or a record, with the totality of all the circumstantial evidence—both digital and real world—both relevant and necessary.

For more information, go to http://www.ncsl.org/issues-research/telecom/uniform-electronic-transactions-acts.aspx.

Electronic Signatures in Global and National Commerce Act

The Electronic Signatures in Global and National Commerce Act (E-SIGN) is a very broad electronic signature law in commerce. On June 30, 2000, President Clinton signed into law the Electronic Records and Signatures in Commerce Act (or Electronic Signatures Act). The president signed the act both electronically and using the more traditional pen-and-ink.

The Electronic Signatures Act (Public Law No: 106-229) went into effect on October 1, 2000 and gives electronic contracts the same weight as those executed on paper. The act has some specific exemptions or preemptions, notably the provision concerning student loans (section 107, (b)(3)).

Although the act enables documents to be signed electronically, the option to do so lies solely with the consumer. In other words, no portion of the act requires you to sign documents electronically, you retain the right to use 'paper & ink' documents at your discretion.

The act specifically avoids stipulating any 'approved' form of electronic signature, instead leaving the method open to interpretation by the marketplace. Any number of methods are acceptable under the act. Methods include simply pressing an *I Accept* button, digital certificates, smart cards and biometrics.

The act does not mandate the use of electronic signature or the type of electronic signature; however, if an entity elects to use electronic signature, it requires a consent be signed to use electronic means for use of communication between two parties. For more information, go to www.ftc.gov/os/2001/06/esign7.htm.

Code of Federal Regulations 21, Part 11; Electronic Records; Electronic Signatures—Food Drug Administration

To date, 21 CFR, Part 11, sets the criteria for electronic signature in use under the Food and Drug Administration.

The regulation defines electronic signature as entry in the form of magnetic impulse or other form of computer data compilation of any symbol or series of symbols executed, adopted, or authorized by a person to be the legally binding equivalent of the person's handwritten signature. It defines a set of electronic signature manifestations where records signed electronically must clearly indicate the name of the signer in print, the date and time when the signature was executed, and the authorship associated with their signature. In addition, the electronic signature must be linked to the record signed, binding the signature to the record and preventing the signature from being copied, excised, or transferred to another record to falsify a signature.

Furthermore, the regulation requires that each signature must be unique to one individual and cannot be shared with anyone else. Electronic signature technology should maintain some level of controls, such as each individual must have a different combination of identification code and password; identification codes or passwords should be periodically changed; the system maintenance should electronically de-authorize lost, stolen, or missing authorization code or password and issue a new authorization code or password; the system should include safeguards to prevent unauthorized access; and the system should be tested periodically to ensure proper functionality.

It also defines electronic signature components. For nonbiometric signatures, the signature must include two distinct components at minimum, such as identification code and password. When a signer logs on for a continuous, uninterrupted session, both components must be met. During this session, if the signer continuously signs documents, at least one component of electronic signature must be met that identifies the signer as the unique individual. If the signer logs with several sessions, then all components of electronic signature must be met.

In regards to sharing a signature, the regulation defines the use of an individual's electronic signature by anyone other than the genuine owner requires collaboration with two or more individuals. For biometric signature, it states the biometric signatures cannot be shared and must be used only by the genuine owner.

For more information on this act, go to www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11.

Code of Federal Regulations, Section 482.24, "Conditions of Participation for Hospitals, Condition of Participation: Medical Record Services (c)(1)(iii)"

Section 482.24 of the Code of Regulations outlines the conditions of participation for hospitals and the conditions of participation for medical record services in the Medicare program. It states, "Authentication may include signatures, written initials, or computer entry." According to CMS'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 electronic signatures. In addition, the organization's governing body must authorize the use of electronic signatures. The use of electronic signatures is acceptable under the Medicare Conditions of Participation. A June 5, 2009, transmittal updated the interpretive guidelines for hospitals related to medical record entries.

Section 482.24 of the Code of Federal Regulation also states, "All patient medical record entries must be legible, complete, dated, timed, and authenticated in written or electronic form by the person responsible for providing or evaluating the service provided, consistent with hospital policies and procedures."

Accordingly:

- The time and date of each entry (orders, reports, notes, etc.) must be accurately documented.
- The hospital must have a method to establish the identity of the author of each entry. This would include verification of the author of faxed orders or entries or computer entries.
- The hospital must have a method to require that each author takes a specific action to verify that the entry being authenticated is his or her entry or that he or she is responsible for the entry, and that the entry is accurate.

The Medicare Conditions of Participation for other care settings have requirements that entries be signed, but acceptable methods of authentication are not specified:

- The Medicare Conditions of Participation for States and Long-Term Care Facilities (42 CFR Ch. IV, Part 483, Subpart A, Section 483.40) require that physicians "write, sign, and date progress notes at each visit and sign and date all orders."
- The Medicare Conditions of Participation for Hospice Care (42 CFR Ch. IV, Subpart C, Section 418.74) require that "entries are made and signed by the person providing the services."
- The Medicare Conditions of Participation for Home Health Agencies (42 CFR, Ch. IV, Section 484.48) require "signed and dated clinical and progress notes."
- The Medicare Conditions of Participation for Rural Primary Care Hospitals (42 CFR Ch. IV, Section 485.638) require "dated signatures of the doctor of medicine or osteopathy or other health care professional."

The Medicare Conditions of Participation 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.

For more information, go to www.cms.hhs.gov/transmittals/downloads/R47SOMA.pdf.

State Laws and Regulations

Healthcare organizations must consult state laws and regulations related to electronic signatures including pharmacy boards that establish additional requirements for signatures related to drug orders, prescriptions, and administration records. States may have also enacted general business laws similar to the federal Uniform Electronic Transactions Act. All state laws for all 50 states are accessible at www.alllaw.com/state_resources. This site is most useful if the citations are known.

Check the state government or legislative Web sites for information. These sites typically have URLs that follow the format: www.[statename].gov.

HIM professionals also should check state HIM Web sites for references, as some have legislative sections that may offer current information related to electronic signature statutes.

Article citation:
AHIMA. "Electronic Signature, Attestation, and Authorship. Appendix B: Laws, Regulations, and Electronic Signature Acts." (Updated October 2013)