Best Practices in Clinical Record Keeping: Signature Authentication

This "Best Practices" guideline provides a summary of requirements and recommendations for authentication of signatures in medical records. As a provider of clinical services, your chart note is the mechanism for memorializing the interaction with the member during that visit. The signature at the end of the note is a symbol which confirms that the signer authored, reviewed, and approved the content of the entry. A proper signature contributes to the integrity of the note as a legal record. Historically, medical records were maintained on paper and relied on handwritten signatures with all of the inherent legibility problems caused by busy providers. With the advent of electronic medical records (EMR), certain other concerns for validity and integrity of signatures have emerged.

The Centers for Medicare & Medicaid Services (CMS) has laid out the criteria for a valid signature, whether handwritten, stamped, or electronic:

- Services that are provided or ordered must be authenticated by the ordering practitioner;
- Signatures are handwritten, electronic, or stamped (stamped signatures are only permitted in the case of an author with a physical disability who can provide proof to a CMS contractor of an inability to sign due to a disability); and
- Signatures are legible.[1]

Handwritten Signatures

The signature must be legible. This can be achieved with a legible first and last name, a legible first initial and legible last name. Alternatively, an illegible signature or initials over a typed/printed legible identification of the author; illegible signature where the letterhead, addressograph or other information on the page indicates the identity of the signatory; where multiple providers are listed the author of record is specifically identified. A signature logmay be used to associate a provider's name with an illegible signature. The log is typically a typed list of the provider(s) who contribute to the medical record. Each name is tied to the corresponding handwritten signature.[2]

Electronic Signatures

Adoption of EMR systems has caused an evolution in the concepts of the electronic signature (e-signature). At this point in time (2016) there is no single overarching standard for e-signatures. One generally recognized health information technology (HIT) standards organization is The

[1] CMS Complying with Medicare Signature Requirements

[2] HC Pro.com Just Coding News: Outpatient, August 11, 2010

Health Level Seven (HL7) [see sidebar]. HL7 defines "authentication" as "the security process of verifying a user's identity that authorizes the individual to access the system (e.g., the sign-on process)." Whereas "attestation" is "the act of applying an e-signature to the content, showing authorship and legal responsibility for a particular unit of information."[3]

For a signature to be valid, systems and software products must include protections against modifications (e.g. time and date stamp), and administrative safeguards should be applied that correspond to standards and laws, e.g. using signature and secure login functions appropriately. Best practice would include the following elements: full printed name of the author at the end of the entry, date and time, the digitized signature or signature statement, e.g. electronically signed by, signed by, authenticated by, reviewed by, etc. with the author's credentials. For example, "Authenticated by Jane Doe, DC on 10/30/2015 at 1:00 pm". [i,]

The Code of Federal Regulations Title 21 of the Food and Drug Administration provides guidance that define "the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."[4]

Electronic signatures typically found in EMRs include:

- Digitized signature which is an electronic representation of a handwritten signature. It is considered to be the weakest form of signature. The digitized signature can be used by anyone to forge a document.
- E-signatures that use "button, PIN, biometric or token" methodology are more secure and strengthen the integrity of the record since use of the signature is dependent on the user having a unique identifier such as a PIN or user/password combination. This guards against unauthorized use of the signature.
- The strongest e-signature is a "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."[5] This highest level of e-signature effectively "locks" a chart entry and prevents alteration or amendment to the content after the digital signature has been

Health Level Seven International (HL7) "is a not-for-profit, ANSI-accredited standards developing organization dedicated to providing a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services." More here.

[3] Health Level Seven. HL7 EHR System Records Management and Evidentiary Support Functional Profile 2009. Available online at www.hl7.org.

[4] CFR Title 21 http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11

[5] AHIMA http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_045551.hcsp?dDocName=bok1_045551

applied. When using an EMR system, be aware of the level of security and integrity that is built into the system's e-signature.

Summary

- A legible signature provides the best level of integrity of a chart note as a legal record.
- Every provider of service (physician, therapist, medical/chiropractic assistant, etc.) should sign the note documenting their service.
- Electronic signatures (e-signature) have varying levels of security and integrity. Be sure that you are aware of the strength of the e-signature in your EMR system.