ELECTRONIC SIGNATURES ON HEALTH CARE DOCUMENTS

State of Wisconsin / Department of Health Services / Division of Quality Assurance

P-02770 (09/2020)

This publication is offered as a guide for **providers regulated by the Division of Quality Assurance** (**DQA) only** and contains clarification on the use of electronic signatures in those health care settings by identifying requirements for electronic signatures and how they pertain to health records.

BACKGROUND

With the development of electronic recordkeeping, various options exist to electronically obtain and store a health care patient or resident signature for necessary documents. For example:

- The patient or resident could sign a paper document that is scanned and placed into the patient's or resident's electronic file.
- The patient or resident could sign a touchpad signature device, similar to when a person makes a credit card purchase. The use of the signature pad produces a graphic image of the person's signature.
- The patient or resident could independently access his/her electronic record, using a unique User ID and password via a sequence of entries, enter a mark that she/he adopts as his/her signature.
- The patient or resident could submit an email indicating approval or send a picture of a signed document, which can be saved to the patient or resident's electronic file.

QUESTION AND ANSWER

Q: Is there a need for a patient or resident to sign a hard copy release for electronic health care records? If so, must the entity retain the hard copy after scanning the hard copy and incorporating the document into the electronic record?

A: A hard copy release is not required. If a paper (hard copy) release is used, a scanned copy may be substituted as the "original" for retention/ recordkeeping purposes. Wis. Stat. § 137.15 provides for legal recognition of electronic records, signatures, and contracts. The statute specifically recognizes the legal effect and enforceability of signatures and contracts in electronic format. The statute recognizes electronic records as satisfying laws that require a record to be in writing, as well electronic signatures as satisfying laws that require a signature.

Wis. Stat. § 137.11(8) defines "Electronic signature" to include "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." Thus, an electronic signature could be created by scanning a signed document and including the scanned image in the electronic record, including the image from a touchpad signature device, or the entry of a "signature" via use of the consumer's adopted image, symbol, or pin number.

ELECTRONIC SIGNATURE REQUIREMENTS

By following the general electronic signature requirements below, the use of electronic signatures provides a secure alternative to written signatures. These requirements align with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule guidelines.

GENERAL REQUIREMENTS

When using an electronic signature, all of the following requirements must be met:

- The electronic signature must be under the sole control of the rendering provider. Only the rendering provider or designee has the authority to use the rendering provider's electronic signature. Providers are required to maintain documentation that shows the electronic signature that belongs to each rendering provider if a numbering or initial system is used (e.g., what number is assigned to a specific rendering provider). This documentation must be kept confidential.
- The provider is required to have current policies and procedures regarding the use of electronic signatures. The Wisconsin Department of Health Services (DHS) recommends the provider conduct an annual review of policies and procedures with those using electronic signatures to promote ongoing compliance and to address any changes in the policies and procedures.
- The provider is required to conduct or review a security risk analysis in accordance with the requirements under 45 CFR § 164.308(a)(1).
- The provider is required to implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

- The provider is required to establish administrative, technical, and physical safeguards in compliance with the HIPAA Security Rule.

ELECTRONIC HEALTH RECORD SIGNATURE REQUIREMENTS

An electronic health record (EHR) that utilizes electronic signatures must meet the following requirements:

- Meet the certification and standard criteria defined in the Health Information Technology Initial Set of Standards, Implementation Specifications, Certification Criteria for Electronic Health Record Technology Final Rule (45 CFR Part 170) and any revisions including, but not limited to, the following:
  - Assign a unique name and/or number for identifying, tracking user identity, and establishing controls that permit only authorized users to access electronic health information.
  - Record actions related to electronic health information according to the standard set forth in 45 CFR § 170.210.
  - Enable a user to generate an audit log for a specific time period. The audit log must also have the ability to sort entries according to any of the elements specified in the standard 45 CFR § 170.210.
  - Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.
  - Record the date, time, patient identification, and user identification when electronic health information is created, modified, accessed, or deleted. An indication of which action(s) occurred and by whom must also be recorded.
  - Use a hashing algorithm with a security strength equal to or greater than Secure Hash Algorithm 1 (SHA-1), as specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-3 (October 2008), to verify that electronic health information has not been altered. (Providers unsure as to whether or not they meet this guideline should contact their information technology and/or security/privacy analyst.)
- Ensure the EHR provides:
  - Nonrepudiation — assurance that the signer cannot deny signing the document in the future
  - User authentication — verification of the signer's identity at the time the signature was generated
  - Integrity of electronically signed documents — retention of data so that each record can be authenticated and attributed to the signer
  - Message integrity — certainty that the document has not been altered since it was signed
  - Capability to convert electronic documents to paper copy — the paper copy must indicate the name of the individual who electronically signed the form as well as the date electronically signed
- Ensure electronically signed records created by the EHR have the same back-up and record retention requirements as paper records.

SUMMARY

The Wisconsin Statutes recognize the legal effect of electronic signatures and records in transactions where the parties have agreed to conduct the transaction by electronic means. In such transactions, there is not a need for a patient or resident to sign a hard copy or paper document. A binding informed consent health care release may be executed electronically in Wisconsin.

There appears to be no legal requirement for an entity to create and retain a hard or paper copy of an electronically signed release. Entities, however, may have their own policy rationales for retaining copies. A bona fide electronic or hard copy backup is required for all providers. Even if not required, back-up alternatives would represent best practice to preserving or protecting resident or patient information.

Under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, covered entities must implement policies and procedures for authentication and integrity of electronically stored health information. For information regarding HIPAA and HITECH requirements, visit the U. S. Department of Health and Human Services health information privacy websites at:

http://www.hhs.gov/ocr/privacy/ and

http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html