TITLE 317. OKLAHOMA HEALTH CARE AUTHORITY
CHAPTER 30. MEDICAL PROVIDERS-FEE FOR SERVICE
SUBCHAPTER 3. GENERAL PROVIDER POLICIES
PART 1. GENERAL SCOPE AND ADMINISTRATION

317:30-3-4.1. Uniform Electronic Transaction Act

The Oklahoma Health Care Authority enacts the provisions of the Uniform Electronic Transaction Act as provided in this Section with the exception to the act as provided in this Section.

(1) **Scope of Act.** The Electronic Transaction Act applies to an electronic record and an electronic signature created with a record that is generated, sent, communicated, received or stored by the Oklahoma Health Care Authority.

(2) **Use of electronic records and electronic signatures.** The rules regarding electronic records and electronic signatures apply when both parties agree to conduct business electronically. Nothing in these regulations requires parties to conduct business electronically. However, should a party have the capability and desire to conduct business electronically with the Oklahoma Health Care Authority, then the following guidelines must be adhered to:

(A) Only employees designated by the provider's agency may make entries in the ~~client's~~ member's medical record. All entries in the ~~client's~~ member's medical record must be dated and authenticated with a method established to identify the author. The identification method may include computer keys, Private/Public Key Infrastructure (PKIs), voice authentication systems that utilize a personal identification number (PIN) and voice authentication, or other codes. Providers must have a process in place to deactivate an employee's access to records upon termination of employment of the designated employee.

(B) When PKIs, computer key/code(s), voice authentication systems or other codes are used, a signed statement must be completed by the agency's employee documenting that the chosen method is under the sole control of the person using it and further demonstrate that:

(i) A list of PKIs, computer key/code(s), voice authentication systems or other codes can be verified;

(ii) All adequate safeguards are maintained to protect against improper or unauthorized use of PKIs, computer keys, or other codes for electronic signatures; and

(iii) Sanctions are in place for improper or unauthorized use of computer key/code(s), PKIs, voice authentication systems or other code types of

electronic signatures.

(C) There must be a specific action by the author to indicate that the entry is verified and accurate. Systems requiring an authentication process include but are not limited to:

(i) Computerized systems that require the provider's employee to review the document on-line and indicate that it has been approved by entering a unique computer key/code capable of verification;

(ii) A system in which the provider's employee signs off against a list of entries that must be verified in the member's records;

(iii) A mail system that sends transcripts to the provider's employee for review;

(iv) A postcard identifying and verifying the accuracy of the record(s) signed and returned by the provider's employee; or

(v) A voice authentication system that clearly identifies author by a designated personal identification number or security code.

(D) Auto-authentication systems that authenticate a report prior to the transcription process do not meet the stated requirements and will not be an acceptable method for the authentication process.

(E) Records may be edited by designated administrators within the provider's facility but must be authenticated by the original author. Edits must be in the form of a correcting entry which preserves entries from the original record. Edits must be completed prior to claims submission or no later than 45 days after the date of service, whichever is later.

(F) Use of the electronic signature, for clinical documentation, shall be deemed to constitute a signature and will have the same effect as a written signature on the clinical documentation. The section of the electronic record documenting the service provided must be authenticated by the employee or individual who provided the described service.

(G) Any authentication method for electronic signatures must:

(i) be unique to the person using it;

(ii) identify the individual signing the document by name and title;

(iii) be capable of verification, assuring that the documentation cannot be altered after the signature has been affixed;

(iv) be under the sole control of the person using it;

(v) be linked to the data in such a manner that if the data is changed, the signature is invalidated; and

(vi) provide strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid.

(H) Failure to properly maintain or authenticate medical records (i.e., signature and date entry) may result in the denial or recoupment of ~~Medicaid~~ SoonerCare payments.

(3) **Record retention for provider medical records.** Providers must retain electronic medical records and have access to the records in accordance with guidelines found at OAC 317:30-3-15.

(4) **Record retention for documents submitted to OHCA electronically.**

(A) The Oklahoma Health Care Authority's system provides that receivers of electronic information may both print and store the electronic information they receive. The Oklahoma Health Care Authority is the custodian of the original electronic record and will retain that record in accordance with a disposition schedule as referenced by the Records Destruction Act. The Oklahoma Health Care Authority will retain an authoritative copy of the transferable record as described in the Electronic Transaction Act that is unique, identifiable and unalterable.

(i) **Manner and format of electronic signature.** The manner and format required by the Oklahoma Health Care Authority will vary dependant upon whether the sender of the document is a ~~recipient~~ member ~~(client)~~ or a provider. In the limited case where a provider is a client, the manner and format is dependent upon the function served by the receipt of the record. In the case the function served is a request for services, then the format required is that required by a recipient. In the case the function served is related to payment for services, then the format required is that required by a provider.

(ii) **Recipient format requirements.** The Oklahoma Health Care Authority will allow ~~recipients~~ members to request ~~Medicaid~~ SoonerCare services electronically. An electronic signature will be authenticated after a validation of the data on the form by another database or databases.

(iii) **Provider format requirements.** The Oklahoma Health Care Authority will permit providers to contract with the Oklahoma Health Care Authority, check and amend claims filed with the Oklahoma Health Care Authority, and file prior authorization requests with

the Oklahoma Health Care Authority. Providers with a social security number or federal employer's identification number will be given a personal identification number (PIN). After using the PIN to access the database, a PIN will be required to transact business electronically.

(B) Providers with the assistance of the Oklahoma Health Care Authority will be required to produce and enforce a security policy that outlines who has access to their data and what transaction employees are permitted to complete as outlined in the policy rules for electronic records and electronic signatures contained in paragraph (2) of this section.

(C) Third Party billers for providers will be permitted to perform electronic transaction as stated in paragraph (2) only after the provider authorizes access to the provider's PIN and a power of attorney by the provider is executed.

(5) ~~**Time**~~ **Time and place of sending and receipt.** The provisions of the Electronic Transaction Act apply to the time and place of receipt with the exception of a power failure, Internet interruption or Internet virus. Should any of the exceptions in this paragraph occur, confirmation is required by the receiving party.

(6) **Illegal representations of electronic transaction.** Any person who fraudulently represents facts in an electronic transaction, acts without authority, or exceeds their authority to perform an electronic transaction may be prosecuted under all applicable criminal and civil laws.