**Section 120.95 Electronic Signatures**

a) Electronic signature or computer-generated signature codes are acceptable as authentication of record content.

b) In order for a provider or ISC agency to employ electronic signatures or computer-generated signature codes for authentication purposes, the provider or ISC agency must adopt a policy that permits authentication by electronic or computer-generated signature.

c) At a minimum, the electronic or computer-generated signature policy shall include adequate safeguards to ensure confidentiality of the codes, including, but not limited to, the following:

1) Each user must be assigned a unique identifier that is generated through a confidential access code.

2) The provider or ISC agency must certify in writing that each identifier is kept strictly confidential. This certification must include a commitment to terminate a user's use of a particular identifier if it is found that the identifier has been misused. "Misused" shall mean that the user has allowed another person or persons to use their personally assigned identifier, or that the identifier has otherwise been inappropriately used.

3) The user must certify in writing that the user is the only person with user access to the identifier and the only person authorized to use the signature code.

4) The provider or ISC agency must monitor the use of identifiers periodically and take corrective action as needed. The process by which the provider or ISC agency will conduct monitoring shall be described in the electronic or computer-generated signature policy.

d) A system employing the use of electronic signatures or computer-generated signature codes for authentication shall include a verification process to ensure that the content of authenticated entries is accurate. The verification process shall include, at a minimum, the following provisions:

1) The system shall require completion of certain designated fields for each type of document before the document may be authenticated, with no blanks, gaps, or obvious contradictory statements appearing within those designated fields. The system shall also require that correction or supplementation of previously authenticated entries shall be made by additional entries, separately authenticated, and made subsequent in time to the original entry.

2) The system must make an opportunity available to the user to verify that the document is accurate and the signature has been properly recorded.

3) The provider or ISC agency must periodically sample records generated by the system to verify the accuracy and integrity of the system.

e) Each document generated by a user must be separately authenticated.

(Source: Added at 48 Ill. Reg. 5279, effective March 21, 2024)