**Section 132.85 Recordkeeping**

a) The provider shall maintain records, including but not limited to the following:

1) Documents required for cost reporting and audit purposes as per the executed contract between the provider and the public payer;

2) Service billing files;

3) Clinical records as defined in Section 132.100; and

4) Individual client information, including representative payee, trust beneficiary and resource availability; and

5) all other documents as required in this Part.

b) Required records shall be retained for a period of not less than 6 calendar years from the date of service, except that if an audit is initiated within the required retention period the records shall be retained until the audit is completed and every exception resolved. This provision is not to be construed as a statute of limitations.

c) Required records shall be readily available for inspection, audit and copying during normal business hours by personnel representing the Certifying State Agency, the public payer, HFS, or the Centers for Medicare and Medicaid Services (CMMS), U.S. Department of Health and Human Services. Reviewing personnel shall make all attempts to examine such records without interfering with the delivery and documentation of services.

d) The compilation and storage of and accessibility to client information and clinical records shall be governed by written policies and procedures, in accordance with the Confidentiality Act, HIPAA and HITECH.

e) Clinical records and other client information shall be secured from theft, loss, or fire.

f) Electronic signature or computer-generated signature codes are acceptable as authentication of record content when compliant with the following requirements:

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

2) At a minimum, the policy shall include adequate safeguards to ensure confidentiality of the codes, including, but not limited to, the following:

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

B) The provider shall certify in writing that each identifier is kept strictly confidential. This certification shall 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 his or her personally assigned identifier or that the identifier has otherwise been inappropriately used.

C) The user shall certify in writing that he or she is the only person with user access to the identifier and the only person authorized to use the signature code.

D) The provider shall monitor the use of identifiers periodically and take corrective action as needed. The process by which the provider will conduct monitoring shall be described in the policy.

3) 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:

A) 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.

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

C) The provider shall periodically sample records generated by the system to verify the accuracy and integrity of the system.

4) Each report generated by a user shall be separately authenticated.

(Source: Amended at 36 Ill. Reg. 18582, effective December 13, 2012)