



STATE OF TENNESSEE
DEPARTMENT OF FINANCE AND ADMINISTRATION
DIVISION OF INTELLECTUAL DISABILITIES SERVICES
ANDREW JACKSON BUILDING, 15TH FLOOR
500 DEADERICK STREET
NASHVILLE, TN 37243

TITLE: Electronic Records and Signature Policy

POLICY #: # P- 022

- A. PURPOSE:** The purpose of this policy is to define general requirements for the acceptable use of electronic records and electronic signatures by contracted providers of the Division of Intellectual Disabilities Services (DIDS) including Home and Community Based Services (HCBS) waiver providers and other providers of DIDS-funded community services. The intent of this policy is to permit and encourage the use of electronic health records (EHRs) and electronic business records, while also ensuring that providers are compliant with all applicable federal and state laws and regulations, policies and interpretive guidance, including but not limited to those referenced herein.
- B. AUTHORITY:** Electronic Signatures in Global and National Commerce Act, "Consumer Consent Provision" Section 101(c)(1)(C)(ii); Health Insurance Portability Accountability Act (HIPAA) of 1996; Section 1915(c) of the Social Security Act (Medicaid Waivers); Tennessee Code Annotated Section 33-3-101 et. seq.; and Tennessee Code Annotated Section 47-10-107.
- C. APPLICABILITY:** This policy applies to HCBS waiver providers and providers of DIDS funded community services that elect to utilize an electronic records and/or electronic signature process for service recipients' records and other records related to the provision of such services (e.g., personnel records, training records, subcontracts).
- D. DEFINITIONS:**
1. **Electronic signature** means 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. Examples of an electronic signature include a name at the end of an email or clicking a button or downloading content to indicate acceptance of a transaction or certain terms and conditions.
 2. **Electronic Health Record (EHR)** means an aggregate electronic record of health-related information on an individual that is created and gathered cumulatively across more than one health care organization. This record may be consulted by licensed clinicians and staff involved in the individual's health and care.
 3. **HCBS waiver or waiver** means a Home and Community Based Services waiver for persons with mental retardation that includes the following;
 - a. Home and Community Based Services Waiver for the Mentally Retarded and Developmentally Disabled (#0128.R04) and any amendments thereto;

- b. Home and Community Based Services Waiver for Persons with Mental Retardation (#0357.R02) and any amendments thereto; and
 - c. Self-Determination Waiver (#0427.R01) and any amendments thereto.
4. **Center for Medicare/Medicaid Services (CMS):** The United States federal agency which administers Medicare, Medicaid, and the Children's Health Insurance Program.
 5. **Health Information Portability and Accountability Act (HIPAA):** A Federal law enacted by the United States Congress in 1996 to address the security and privacy of health data.
 6. **Administrative safeguards** are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect EHR and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
 7. **Physical safeguards** are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
 8. **Technical safeguards** means the technology and the policy and procedures for its use that protect EHR and control access to it.

E. DESCRIPTION OF POLICY

1. The creation, presentation, retention, and exchange of 1) business records; and 2) service recipient health information (including information pertaining to eligibility to receive, delivery of, and payment for home and community based services) is permitted in an electronic format.
2. Providers electing to maintain health information in an EHR must maintain written or electronic policies and procedures to prevent, detect, contain and correct security violations, and guide in the operations and maintenance of EHR systems to ensure information integrity, availability and security. These policies and procedures must be:
 - a. Retained for 6 years from the date of creation or the date when last in effect, whichever is later.
 - b. Available to those persons responsible for implementing the policies and procedures.
 - c. Reviewed and updated as needed in response to environmental, legislative, or operational changes affecting the security of the EHRs.
3. EHRs are considered all or part of the service recipients' confidential main file. EHRs must meet all standards established by federal and state law and regulation, policies and interpretive guidance.
4. EHRs must be maintained on a secure system, and all applicable administrative, physical and technical safeguards must be in place to ensure the security and privacy of all health records.
5. Required employee access to recipient or employee personnel file information may be accessed in a facility or service site either through a paper file system, electronic file system, or a combination of both. If records may be accessed from a residential facility, supported living site or day services facility electronically and/or printed on hard copy as needed or requested, it is not necessary to produce the information on paper until needed and/or requested, except as set forth below in (6) below.
6. It is the provider's responsibility to ensure ready access to recipient information in a timely manner. If an agency utilizes EHRs as a means to store recipient file information, there must be an established protocol to help ensure ready access to needed recipient information in the event that technology does not function properly. As part of this protocol, providers are required to maintain *at a minimum* a hard copy of the current Individual Support Plan and the Health Care Passport in the residential facility or supported living where the recipient lives and in any other licensed facility where services are delivered, including day services facilities.

7. An electronic signature is recognized as a legitimate method for authentication of an entry in the record, so long as it comports with definitions and standards set forth in federal and state law and regulation and this policy.
8. The acceptable use of an electronic signature must:
 - a. Be unique to the user, under his or her sole control, and verify the identity of the signer (or "authenticate the user") to a person receiving or reviewing the signed record. A simple typed signature, symbol or mark does not satisfy this requirement if persons other than the signer could also have typed such signature, or provided such symbol or mark.
 - b. Ensure that what was signed cannot be altered. A compliant system of electronic signature must be able to detect changes to the electronic record made after it was electronically signed. Any change to the document once it has been signed invalidates the signature.
 - c. Provide non-repudiation, meaning that the system of electronic signature should not permit the signer to successfully deny that he willingly and intentionally signed the document, or is not responsible for information contained in the signed record. This may be accomplished, for example, through use of an acknowledgement that the user must click in order to sign the record.
9. Providers electing to utilize electronic signatures must adopt a usage policy incorporating at a minimum, the following information:
 - a. Definition of electronic signature;
 - b. How the provider's system of electronic signature comports with each of the elements of acceptable use specified above;
 - c. Acknowledgement that the electronic signature is legally enforceable; and
 - d. Retention of an electronic document with an electronic signature will satisfy record retention requirements.

F. **ATTACHMENTS**: Not applicable

G. **PREVIOUS POLICY**: Not applicable

H. **DATE APPROVED BY TENNCARE**: September 24, 2010

I. **POLICY APPROVAL**



Signature of Assistant Commissioner
Office of Policy and Rule Development

9/28/2010
Date



Signature of Deputy Commissioner
Division of Intellectual Disabilities Services

9-28-10
Date