

POLICY AND PROCEDURE

REACH for Tomorrow

Electronic Signature and Authentication Policy

Partial Hospitalization Program (PHP)

Effective Date: 08/15/2025

Approved By: Director of Medical and Clinical Services

Review Schedule: Annually or as Needed

Applies To: All Programs — Outpatient MH/SUD, IOP, PHP, and Integrated Primary Care/Behavioral Health

Purpose

To establish standards for the use of electronic signatures and authentication within the electronic health record (EHR). This policy ensures that electronic documentation is secure, legally valid, and compliant with regulatory and accreditation requirements.

Policy

The organization authorizes the use of electronic signatures for clinical documentation, orders, and administrative records within approved electronic systems. Electronic signatures serve as the legal equivalent of handwritten signatures and confirm the identity of the individual completing the documentation.

Definition of Electronic Signature

An electronic signature is a unique digital identifier used by an authorized user to sign electronic documents within an approved system. The signature verifies authorship and confirms that the individual reviewed and approved the information contained in the record.

Authentication Requirements

All staff using electronic documentation systems must authenticate their identity using secure login credentials. Authentication methods may include:

- Unique username and password
- Multi-factor authentication when available
- System-based identity verification

POLICY AND PROCEDURE

REACH for Tomorrow

User credentials must not be shared with others.

Authorized Users

Only authorized personnel who have received appropriate system access and training may apply electronic signatures. Authorization levels are determined based on staff role, scope of practice, and organizational credentialing procedures.

Electronic Signature Use

Electronic signatures may be used for:

- Clinical progress notes
- Treatment plans and reviews
- Medication orders and documentation
- Discharge summaries
- Incident reports
- Administrative documentation when appropriate

Signature Integrity

Once an electronic signature is applied, the record becomes part of the permanent clinical record. Any modifications must follow established amendment procedures and must not obscure the original documentation.

Late Entries and Amendments

If additional documentation is required after the original entry:

- A clearly labeled late entry or amendment must be created
- The date and time of the new entry must be recorded
- The author must electronically sign the new entry

Security Responsibilities

Staff are responsible for protecting the security of electronic systems by:

- Logging out of systems when not in use
- Protecting passwords and access credentials

POLICY AND PROCEDURE

REACH for Tomorrow

- Reporting suspected unauthorized access immediately

Audit and Monitoring

Electronic documentation systems maintain audit trails that record:

- User access
- Document creation and modification
- Electronic signature application

Audit trails may be reviewed periodically to ensure compliance and data integrity.

Training

Staff receive training on proper electronic documentation, authentication procedures, and confidentiality protections prior to receiving system access.

Compliance

Electronic signature practices must comply with applicable regulations and standards including:

- HIPAA security requirements
- Organizational documentation policies
- Accreditation standards for record integrity and authentication