Digital Signatures Policy and Procedure

Policy

It is the intent of Search for Change, Inc. to ensure all agency service documentation remains in compliance with applicable state and federal statutes. This policy is in no way intended to have the effect or altering the efficacy of our Corporate Compliance program in keeping the agency in compliance with governing statutes and regulations.

The agency recognizes the change in the healthcare industry from a paper-based system of service documentation to that of an electronic format. Search for Change, Inc. approves the use of "digital" signatures wherever staff signatures are required for billing/service documentation purposes.

It shall be the responsibility of the Chief Executive Officer and staff designated by the Chief Executive Officer to develop, and execute all internal operational procedures in accordance with state and federal law with regard to the implementation of "digital" signatures in electronic record keeping.

Procedure

Digital signatures will be used in the documentation of provided services. The primary use of the digital signature shall be in the PrecisionCare electronic health record.

Use of Strong Passwords

Each staff member shall develop a "strong" password that must be different from your network and Precision Care log in passwords.

A "strong" password requires:

- A minimum of 8 characters
- At least 1 character must be an upper-case alpha character (A-Z)
- At least 1 character must be a lower-case alpha character (a-z)
- At least 1 character must be a number (0-9)
- At least 1 character must be a special character

The electronic system will require passwords be changed every six months. In the event that a staff member enters a password incorrectly, the system will allow only 3 attempts and then the staff member will be locked out of the system and will need to contact a systems administrator.

Staff members will be required to digitally sign the completed document creating an electronic fingerprint on the document. The system will cue the user to enter their strong password and to indicate the validation that they understand the intent of the electronic document they are signing. The system will then record the date, time, and employee name making an inalterable "stamp" on the record electronically.

No electronic document of services shall be considered executed until it has been digitally validated, signed, and subsequently "stamped" within the system.

Inalterable Documentation/Compliance Integrity

Upon the staff using their strong password to digitally sign the document, the document will then contain an inalterable electronic fingerprint and timestamp. Any edits to the document after it was digitally signed must be approved by the Compliance Officer and explained in a separate addendum

All staff members are expressly prohibited from sharing any electronic passwords. Supervisors are prohibited from knowing, or requesting a staff member's password. In the event an employee forgets their password they are required to report this to the Corporate Compliance Officer and/or designated Administrative Supervisors who will ensure the system is re-set allowing the employee to create a new password.

Staff members who knowingly share their passwords shall be considered in violation of the agency's Corporate Compliance Program and Policies. They will be subject to the same disciplinary measures described in the policy including the possibility of termination. Any staff member who uses another employee's password for the purposes of logging into, or digitally signing service documentation shall be considered guilty of committing forgery.

Contemporaneous Documentation

This is the period of time from when a service is delivered to the time it is documented. Search for Change, Inc. defines the time period between service delivery and service documentation as a maximum of 10 calendar days. Once the 10 calendar days' time period has passed it is too late to document the service and the service will not be billed. This is only applicable to billing notes in Medicaid Billing Programs. For Non-Medicaid Billing programs and notes that are not utilized for billing, the contemporaneous period is a maximum of 30 calendar days. Service Plans and Service Plan Reviews must be digitally signed, certified, and "stamped" prior to or on the exact date the document is due. Service Plans and Reviews should not be digitally signed and "stamped" after established due dates.

In the event that the electronic system is not available employees are to document the service using the agency paper record system and sign and date the note. This is time limited and requires approval from the Compliance Officer Once the electronic system is available these notes may be entered outside of the contemporaneous time period using the "billing note exception" modality in PrecisionCare with the Compliance Officer prior approval.

Retention of Records/Audit

All digital records shall be retained for the legally required time period. For Medicaid documentation related to service delivery that is no less than 3 years on site and 7 years with our document storage company, totaling 10 years of record retention. In the event of a service or billing audit records shall be made available electronically at the convenience of auditor by the Compliance Officer.

Auditors may require service documentation be printed in hard copy for review. The agency shall make copies available to any auditor upon request. Hard copies shall print with the date and signature timestamp clearly present on the document.

The Compliance Officer, or their designee, shall be the liaison with PrecisionCare engineers in the event of issues with the system, or an audit situation requiring information from the engineers specifically.

Any questions regarding the policy may be directed to the Corporate Compliance Officer who shall be accountable for receiving any reports of abuse of the system as well as responding to questions.

The Corporate Compliance Officer, or their designee, shall be the liaison with PrecisionCare engineers in the event of issues with the system, or an audit situation requiring information from the engineers specifically.

Date Adopted: 4/19
Reviewed/Revised: 10/22, 2/24, 3/24