POLICY

Renew Home Health staff may use electronic signatures on all computer-generated documentation. An electronic signature will serve as authentication on patient record documents generated via the organization's EMR application.

Purpose:

To utilize current technology in the provision of patient care

Responsibility:

All personnel

Procedure:

1. Renew Home Health staff may create *patient* documentation via computer system.
2. For the purpose of the electronic medical record, and documents printed from the electronic medical record, the employee's use of an Electronic Signature Passcode after authenticating with her/his system Log In Authentication Password will serve as her/his legal signature.
3. The organization-based application administrator will issue each employee a system User Name and a temporary password. The user will create a new password upon initial log in to the organization's EMR application.
4. The employee will generate an Electronic Signature Passcode that will only be accessible to her/him.
5. Each user will be required to change her/his Log In Authentication Password:
    a. upon her/his password being reset by an organization-based application administrator;
    b. every 60 days; or
    c. at the employee's discretion.
6. If an Electronic Signature Passcode must be reset, the user can reset her/his own Electronic Signature Passcode or contact organization's Customer Support for help to reset the Electronic Signature Passcode with employee authentication.
7. After completion of a clinical document, the clinician must enter her/his Electronic Signature Passcode to submit the clinical document to the case manager.
8. Each employee documenting electronically in the electronic medical record will be required to sign an Electronic Documentation & Signature Authenticity Agreement. (See appendix A).This Agreement will require that she/he:
    a. ensure the security of his/her Log In Authentication Password and Electronic Signature Passcode information, which may not be shared with anyone;
    b. exit the electronic medical record software when the computer will not be used for clinical documentation or is out of her/his possession, and at the end of each working day; and
    c. review all documentation prior to submission.

9. Each employee will review documentation and make necessary corrections per organization policy to documents returned by a case manager, at which time the clinician will be required to reenter the Electronic Signature Passcode to re-submit the documentation.
10. In the event of system downtime that results in the employee's inability to use the electronic documentation system, the employee will complete records manually.
11. Each user must keep her/his Log In User Name, Authentication Password, and Electronic Signature Passcode confidential. Only the user her/himself and an organization-based administrator may reset a user's Log In Authentication Password.
12. Upon termination of employment, the administrator will immediately disable the employee user's credentials to prevent access to the electronic medical record.

(Appendix A):

Electronic Documentation & Signature Authenticity Agreement

I understand that Renew Home Health staff may use electronic signatures on all computer-generated documentation. An electronic signature will serve as authentication on patient record documents and other organization documents generated in the electronic system.

For purposes of the computerized medical record and other organizational documentation, I acknowledge that the combined use of my Electronic Signature Passcode and Log In Authentication Password will serve as my legal signature. I further understand that an organization-based administrator will issue my initial employee password and that I will create an Electronic Signature Passcode within the software application.

Log In Authentication Passwords must be updated every 60 days by the user, as well as on an as-needed basis in the event system security is breached. I understand that prior to exporting documentation to the organization server, I must review and authenticate, by use of electronic signature, my documentation on the field-based or office computer. I understand that I am responsible for the security and accuracy of information entered into my organization's EMR application, and as such, I will:

- not share or otherwise compromise my electronic signature credentials (Log In Authentication Password or Electronic Signature Passcode);
- exit the online application at the end of each working day or whenever the computer is not in my immediate possession;
- not save my Log In Authentication Password and Electronic Signature Passcode on the computer, but will enter them upon each access of the application; and
- review all of my documentation online prior to submitting to the organization.

Employee Signature	Date
Witness Signature	Date