**Purpose**

To facilitate the usage of electronic signatures for medical records throughout the clinical operations of Ohio Living.

**Policy**

Electronic signature, an automated function which replaces a handwritten signature with a system generated signature statement, will be utilized for medical records as a means for authentication of transcribed documents, computer generated documents and/or electronic entries. System generated electronic signatures are considered legally binding as a means to identify the author of medical record entries and confirm that the contents are what the author intended.

**Procedure**

1. ELECTRONIC SIGNATURES ALLOWED – The following are all types of electronic signatures that can be utilized:
   1. All users will have a unique ID and password which will act as the users electronic signature. The password is not viewable on any screen.
   2. Entries, orders and electronically created documents will bear the electronic signature statement: “created by, verified by, ordered by or signed by “which acts as the users electronic signature for that entry, document or order.
   3. Digitized signature (actual signature converted to electronic image)
      1. The author of the entry will review/validate the entry prior to applying electronic or digitized signature.
2. USAGE OF ELECTRONIC SIGNATURE
   1. A document and/or entry signed electronically will include a digitized signature and/or a signature statement with the authenticator’s name, date and time the document or entry was signed.
   2. The electronic signature will be treated as a written signature.
3. SECURITY
   1. Every user authorized to utilize electronic signatures will be the only one who has access to his/her signature codes, that the electronic signature will be legally binding and that passwords and/or ID numbers will not be shared.
   2. User’s who use electronic signature based upon the use of user IDs and passwords as described in this policy, shall use additional controls to ensure the security and integrity of each user’s electronic signature:
      1. Follow Ohio Living Information Technology procedures to electronically unauthorize lost, stolen, missing or otherwise compromised documents or devices that bear or generate identification code or password information.
   3. The Private Health Information (PHI) report is a computer-generated, time-stamped audit trail that records independently the date and time of user entries, including actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information. Audit trail documentation shall be retained for a period at least as long as that required for the medical record and shall be made available as needed upon request.

**References/Citations**

AHIMA e-HIM Workgroup: Best Practices for Electronic Signature and Attestation. "Electronic Signature, Attestation, and Authorship (Updated)." *Journal of AHIMA* 80, no.11 (November-December 2009): expanded online edition.

<http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_045551.hcsp?dDocName=bok1_045551>

Center for Medicaid and State Operations/Survey and Certification Group, Survey and Certification Letter: Ref: S&C-05-14, January 13, 2005

Medicare Program Integrity Manual, Chapter 3: section 3.4.1.1 Documentation Specifications for Areas Selected for Prepayment or Post payment MR   
(Rev. 248; Issued: 03-28-08; Effective Date: 09-03-07; Implementation Date: 04-28-08)