Policy Number: HC-32	Page: 1	Of: 2
Title: Electronic Signatures		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A) ELECTRONIC SIGNATURES

Electronic signatures may be utilized at HCBDD by both employees and providers. Electronic signatures are legally binding as a means to identify the author and to confirm that the contents are what the author intended.

Audience

Employees using electronic signatures; managers

Authority

ORC § 1306 Ohio Uniform Electronic Transactions Act

ORC § 304 Electronic Records and Signatures for Counties

ORC § 9.01 Official Records – Preserving and Maintaining

ORC § 117.111 State Audits shall review method, accuracy and effectiveness of electronic signature security procedures

1) Definitions

a) Electronic Signature, as defined by the Ohio Revised Code, 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.

b) Electronic facsimile. A computer image, such as one maintained in an electronic document imaging system, of a conventionally signed document is not an electronic signature. Rather, the electronic facsimile is legally equivalent to the original, traditionally signed document.

2) Security

a) **Confidentiality statement**. Anyone authorized to utilize electronic signature will be required to sign a statement attesting that he or she is the only one who has access to his/her signature/ logon password, that the electronic signature will be legally binding and that passwords will not be shared and will be kept confidential.

b) **Passwords**. All users will have their own user ID and password. Passwords must conform to complexity guidelines detailed in Policy 3080 Computer Usage.

c) **Personal Identification Numbers (PIN)/ Secondary Passwords.** PIN numbers and/or secondary passwords may be assigned when possible for use with electronic signatures

to allow for another level of security (this is optional and county specific). PIN numbers or secondary passwords are not viewable on any screen.

d) Vendors, outside agency or providers who have access to using an application requiring an electronic signature based upon the user's ID and password as described in this policy, shall use additional controls to ensure the security and integrity of each user's electronic signature:
   i) Follow loss management procedures to electronically de-authorize lost, stolen, missing or otherwise compromised documents or devices that bear or generate identification code or password information and use suitable, rigorous controls to issue temporary or permanent replacements;
   ii) Use safeguards to prevent the unauthorized use or attempted use of passwords and/or identification codes; and
   iii) Test or use only tested devices, such as tokens or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered.

3) **Creating, Maintaining an Electronic Signature**
   a) Electronic signatures can be used wherever handwritten signatures are used except where stated by a specific law or rule.
   b) All who use a system that uses electronic signatures are required to review their entries.
   c) Once an entry has been signed electronically, the computer system will prevent it from being deleted or altered. If errors are later found in the entry or if information must be added, this will be done by means of addendum to the original entry. The addendum should also be signed electronically and date/time stamped by the computer software.
   d) System specific standards and procedures for use may vary by system and it will be required that the board must establish and maintain system specific procedures for any system which also satisfies other current policies.

4) **Auditing Electronic Signature Procedures**
   The computer software and anyone using the software system must use a secure, 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 record and shall be made available as needed upon request. Any misuse or disregard of electronic signature policy will be reviewed and acted upon by the Superintendent or designee.

5) **Review and Approval Prior to Using Electronic Signatures**
   The HIPAA Security Officer shall review the software utilized for electronic signatures, and other procedures utilized, for compliance with this policy prior to permitting the use of electronic signatures. This review shall be conducted for each transaction to be electronically signed.