ELECTRONIC SIGNATURES POLICY

3.06

Effective Date: 07/18

Purpose: The purpose of this policy is to establish a foundation for procedures to guide legal and compliant electronic signature processes and to facilitate the use of electronic signatures for health records and supporting documents generated during healthcare operations, validate information accuracy, verify the identification of the authors of electronic health records or other documentation, and to support non-repudiation, contracts, purchasing, and general office administration (such as employee expense). This policy is to ensure neither Barren River District Health Department (BRDHD), its staff, or those we associate with are misrepresented or exposed to any liability or other adverse consequence through the use of an electronic signature.

Failure to comply: This policy applies to all full time, part time, variable hour, and contract employees. This policy also applies to any students, interns, Board members, or volunteers acting in some capacity for the BRDHD. Following the requirements of this policy is essential and any breach may lead to disciplinary action being taken up to and including dismissal per 902 KAR 8:100.

Policy: Per the Federal Electronic Communication Privacy Act of 2000 and the Electronic Signatures in Global and National Commerce Act (E-SIGN), the legal definition of an electronic signature is anything in electronic format which is:

A) Incorporated into or otherwise logically associated with any electronic communication or electronic data; and

B) Purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of a communication or data, the integrity of the communication or data, or both.

Per the KRS 369.101 to 369.120, the Kentucky Information Technology Uniform Electronic Transmissions Act, the legal definition of an electronic signature is “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.”

Forms of Electronic Signatures

The E-SIGN went into effect on October 1, 2000 and gives electronic contracts the same weight as those executed on paper. The act has some specific exemptions or preemptions. Although the act enables documents to be signed electronically, the option to do so lies solely with the consumer. The act specifically avoids stipulating any 'approved' form of electronic signature, instead leaving the method open to interpretation by the marketplace. Any number of methods is acceptable under the act. Methods include simply pressing an 'I Accept' button, digital certificates, smart cards, and biometrics. E-signatures may be implemented using various methodologies depending on the risks associated with the transaction. Examples of transaction risks include: fraud, non-repudiation, and financial loss. The quality and security of the e-signature method should be commensurate with the risk and needed assurance of the authenticity of the signer. Authentication is a way to ensure that the user who attempts to perform the function of an electronic signature is in fact who they say they are and is authorized to "sign".

Using the legal definitions listed above, any of the following methods may be utilized by BRDHD staff to create an electronic signature. Other methods that may be adopted at a later time:

A) A uniquely password-secured BRDHD email account.
B) A digitally certified signature created in approved PDF software.
C) A manual signature captured electronically via a signature pad or similar device.
D) A document utilizing built-in security functions to create unique password protection.

Legal Impact of Electronic Signatures

As stated above, electronic signatures are legal signatures. It is possible to commit yourself or the BRDHD to contracts or other obligations using electronic signatures just as you would use a manual signature. It is possible that an electronic signature could be used in court as evidence of the authenticity of the communication or document if it is separately confirmed that the signature is a means of authenticating the communication or document.

It is the policy of this organization to accept electronic signatures as defined within this policy for author validation of documentation, content accuracy, and completeness with all the associated ethical, business, and legal implications.

As stated in Policy 3.11 - Internet and Information Technology Acceptable Use Policy, you must not share passwords, specifically email passwords, to accounts you may be using as an electronic signature. It is not acceptable to send an email logged in as another person. Both disclosure of a personal password and use of another person's password are potentially serious disciplinary offenses.

Electronic Signature Participation

The requesting department or program will seek approval to implement an e-signature from the applicable records custodian; i.e., a State Program Manager, applicable governing body, or the Kentucky Department of Libraries and Archives. It is the records custodian's responsibility to ensure that the proposed e-signature and method meet the requirements of this policy. In determining whether to

approve an e-signature method, consideration will be given to the systems and procedures associated with using that electronic signature, and whether the use of the electronic signature is at least as reliable as the existing method being used. Should it be deemed necessary by the records custodian, he/she will seek approval from legal counsel and the appropriate information technology office or officer.

A participation agreement is required for providers outside of BRDHD attesting to agree to the scope of this policy and the commitment to safekeeping of user information. The agreement provides acknowledgment of and user intention to uphold organization policies and practices for properly executed electronic signature processes. Completed agreements would include an initial agreement by providers prior to first use with annual agreement renewal thereafter. The agreement should be retained by the initiating department.

Review Requirements

*All hardware and software used to produce an electronic signature for BRDHD staff must be approved and provided by the BRDHD IS Department. The IS Department will review all uses of the electronic signature with an annual risk review.

Forms: None

References: 902 KAR 8:100; Federal Electronic Communication Privacy Act of 2000; Electronic Signatures in Global and National Commerce Act (E-SIGN); KRS 369.101 to 369.120, the Kentucky Information Technology Uniform Electronic Transmissions Act; Policy 3.11 - Internet and Information Technology Acceptable Use Policy;

Contact Persons: Director of Information Systems; Director of Finance; Human Resources Manager; Public Health Director

Policy Origination, Revision, and Review Tracking

Policy Version Number	Origination Date	Description of Revision or Reviewer Name
3.06	01.24.2018	HR Manager – Policy Creation
3.06	10.16.20	IT Manager-reviewed