

POLICY AND PROCEDURES

OFFICE OF STRATEGIC PROGRAMS

Electronic and Digital Signatures for Records Management

Table of Contents

PURPOSE1

BACKGROUND1

POLICY2

RESPONSIBILITIES2

PROCEDURES3

REFERENCES.....3

DEFINITIONS4

EFFECTIVE DATE.....4

 ATTACHMENT 1: How to Sign a Record
 Electronically or Digitally.....5

 ATTACHMENT 2: E-Signature Examples6

PURPOSE

This MAPP establishes policies, procedures, requirements, and responsibilities for the use of electronic and digital signatures for internally generated CDER records.

This MAPP does not identify which documents require signature, or identify best signature methods. CDER staff should refer to their Office’s policies and procedures for specific instructions on how to sign specific documents.

BACKGROUND

During the conduct of its business, CDER staff creates a wide variety of documents requiring signatures. The ability of employees to electronically or digitally sign documents is vital to day-to-day operations. Seamless facilitation of electronic and digital signatures is also a critical component of CDER’s Records Management (RM) program.

An electronic signature is a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

A digital signature is an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

Several statutes govern the use of electronic and digital signatures in the Federal Government. These statutes establish that electronic or digital signatures may not be denied legal effect, validity, or enforceability solely because they are in electronic or digital form. These statutes also specify general requirements for electronic or digital signature to be deemed equivalent to a handwritten signature.

POLICY

- CDER uses electronic or digital signatures whenever possible and appropriate. The signer of each CDER document follows the procedure method based on the level of security necessary for the transaction, to ensure authenticity and to reduce the risk of fraud.
- CDER provides the technology and processes for preserving the integrity of the Electronic or Digital signature of the associated record.
- Electronic and Digital signatures are only supported through the use of the FDA Personal Identity Verification (PIV) card.
- Each electronic and digital signature is unique to one CDER employee and must not be used or shared by anyone else. Each electronic and digital signature explicitly authenticates the employee executing the signature, and displays both the first and last name of the signer, and the time and date the electronic or digital signature was applied.
- Each CDER Office defines and documents their processes for which documents require electronic or digital signatures. All electronic and digital signature processes of CDER Offices must adhere to the procedures in this MAPP.
- The electronic and digital signature is considered invalid if the electronic record has been altered or modified after being signed.
- The electronic or digital signature is considered invalid if electronically signed by an expired or repudiated means of authentication, or any other expired electronic signature token, certificate, or Public Key Infrastructure (PKI) device.

RESPONSIBILITIES

Office of Business Informatics (OBI) in the Office of Strategic Programs (OSP)

- Ensures that projects and documents utilizing electronic or digital signatures are in conformance with the policies stated forth in this MAPP and with applicable laws and regulations.

-
- Ensures methods to preserve the integrity of electronically and digitally signed documents.

Assistant Records Liaison Officer (ARLO)

- Provides RM guidance for electronic or digital signature policies throughout CDER.

Document Signer

- Verifies appropriate signature method prior to applying an electronic or digital signature.
- Signs documents according to Office policies and procedures.

CDER Super Office or Office Directors (or designee)

- Defines Office-wide processes for electronic or digital signatures. Ensure the Office electronic procedures are in alignment with this MAPP.
- Ensures associated records reflecting how each signature was created are maintained as per Records Management best practices.
- Ensures staff are trained on the appropriate use of electronic or digital signatures.

CDER Staff

- Follow the electronic and digital signature policies and procedures in this MAPP.

PROCEDURES

1. Super Office or Office Directors (or designee) determines if a record should be signed electronically or digitally.
2. Super Office or Office Director (or designee) communicates document signing protocol and procedures to staff, and ensures appropriate training.
3. Signer receives, reviews, and signs document using the appropriate signature method. (See Attachment 1).

REFERENCES

1. Electronic Signatures in Global and National Commerce Act (E-SIGN) of 2000 – Public Law No. 106-229, 15 U.S.C. 7001, et seq.
2. Government Paperwork Elimination Act (GPEA) of 1998 – Public Law No. 105-277 Title XVII, 44 USC 3504 (as implemented by OMB, Procedures and Guidance, *Implementation of the Government Paperwork Elimination Act*, 65 Fed. Reg 25508-21 (May 2, 2000)).
3. 21 Code of Federal Regulations (CFR) Part 11.

DEFINITIONS

Digital Signature: An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

Digital signatures apply encryption technology, enabling secure transmission of unique identifiers over a network. Digital signatures include a certificate of authority, to ensure the validity of the signature.

Electronic Signature: A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

An electronic signature is not technology-specific; it does not require the use of any particular hardware or software application. Electronic signatures allow for any technology that can authenticate the signer and the signed document. Electronic signatures are used to approve and sign electronic documents.

Public-Key Infrastructure (PKI) Technology: A digital signature technology that requires the use of two 'keys,' one private to the person signing in this fashion and one non-private key available to the counterparty to the transaction using the digital signature. The private key and the non-private key are mathematically related, but it is impossible to guess the private key from the public key. Therefore, the technology authenticates the signer and prevents identity fraud. CDER staff have PKI keys embedded in their PIV cards.

Records: All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor. Records are evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government, because of the informational value of data in them. The term 'Records' does not include library and museum material made or acquired and preserved solely for reference or exhibition purposes, or duplicate copies of records preserved only for convenience as per 44 U.S.C.3301.

EFFECTIVE DATE

This MAPP is effective upon date of publication.

ATTACHMENT 1: How to Sign a Record Electronically or Digitally

If using a CDER Informatics system:

1. Log on to the pertinent FDA system with the established Single Sign On (SSO).
2. Follow system prompts to check in, or upload, a document or record.
3. Sign document using SSO authentication.

Note: If more guidance is needed, consult the support documentation for the system you are using.

If using Adobe Acrobat without embedded signature field:

1. Review record before signing.
2. Follow adobe instructions to “Sign and Certify.”
3. Enter PIV card pin number when prompted.

If using Adobe Acrobat with embedded signature field (fillable form):

1. Review record before signing.
2. Click on the embedded signature field to sign.
3. Enter PIV card pin number when prompted.

Notes:

- i) *FDA-secured Public Key Infrastructure (PKI) credentials are embedded in the FDA-issued PIV cards. The electronic certificate embedded on each employee’s PIV card creates valid electronic or digital signatures. CDER staff are authorized to sign records with electronic or digital signatures, using PIV cards in conjunction with office automation applications available in CDER.*
- ii) *The exact steps to sign a document in Adobe may differ, depending on the version of Adobe installed on the computer, or if a fillable form is being used.*

If the system does not embed an electronic or digital signature when employees follow the above steps, employees should contact FDA ERIC at ERIC@fda.hhs.gov.

ATTACHMENT 2: E-Signature Examples

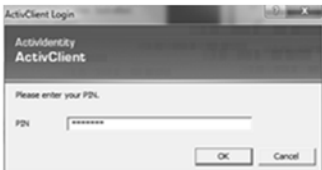

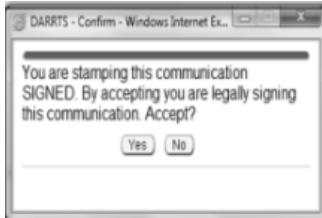
E-Signatures are computer data compilations of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Symbols:

- A typed name, either typed at the end of an e-mail message by the sender, or typed into a signature block on a website form by a party.
- A digitized image of a handwritten signature that is attached to an electronic record.
- A secret, such as a secret code, password, or PIN, used by a person to sign the electronic record.
- A digital signature.
- A biometrics-based identifier, such as a fingerprint, a voice print, or a retinal scan.

Processes:

- The process of clicking a consent button, such as clicking an “I Agree” button.
- The process of using a private key and applicable software to apply an electronic or digital signature.
- The process of scanning and applying a fingerprint.

Signature Type	Process Definition	Sample Screenshot Image	
PDF/PIV Card Signature	User opens a .pdf document, applies an Adobe digital signature, and provides PIV authentication.		
System Generated Authenticated Signature (Informatics Platform; Panorama and DARRTS)	User applies an electronic signature available in a system that is authenticated through network sign-on.		<p>This is a representation of an electronic record that was signed electronically and this page is the manifestation of the electronic signature.</p> <p>/s/ [Redacted] 12/08/2015</p>

Sample processes used to electronically sign documents electronically in CDER.