Electronic Signatures, Transmission and Storage: Overview of Notice H 2020-04

Heather Sievers

Nan McKay AND ASSOCIATES, INC.

Experience — Leadership — Collaboration

1

Purpose

- Provides guidance to HUD multifamily assisted housing industry partners on electronic signatures, electronic transmission, and electronic storage of documents and forms required by HUD's Office of Asset Management and Portfolio Oversight (OAMPO)
- Industry partners include:
  - Owners and management agents (O/A) of HUD multifamily assisted housing properties;
  - Service providers; and
  - HUD and Contract Administrator (CA) staff

2

2

Effective Date

- Issued May 26, 2020
- Effective immediately
- May implement at any time

3

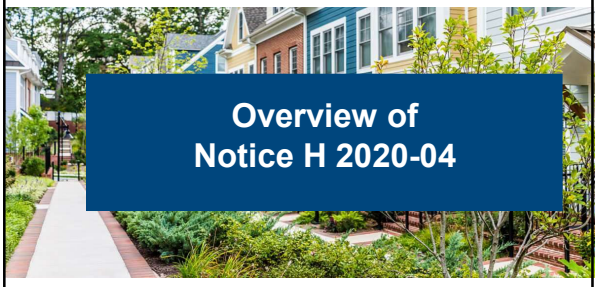
3

Reference

- Much of the information in this Notice is taken from "Use of Electronic Signatures in Federal Organization Transactions"
  - Issued by the Federal Chief Information Officer (CIO) Council in January 2013
- HUD encourages O/As to review this document along with the Notice

4

4



Overview of Notice H 2020-04

5

5

Notice H 2020-04

- Permits, but does not require:
  - Multifamily O/As to use electronic signatures (e-signatures)
  - Electronic transmission and storage of files

6

6

Other Laws

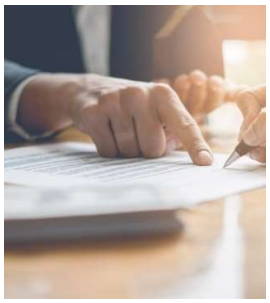
- O/As choosing to use electronic signatures, transmission, and/or storage of documents must comply with federal, state, and local laws

7

7

Wet Signatures & Paper Documents

- O/As adopting the Notice must provide applicants and tenants the option to use wet signatures and paper documents upon request

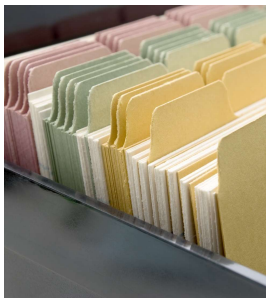


8

8

Required Documents

- This Notice does not change the nature or use of required documents



9

9

Example

- O/A can accept a tenant's self-certification if the information can't be verified by other acceptable methods
- But the document may be submitted on signed paper and/or transmitted to the O/A electronically

10

Applicable Programs

- Section 8 programs, including:
  - New Construction
  - State Agency Financed
  - Substantial Rehabilitation
  - Supportive Housing for the Elderly with project-based Section 8 (Section 202/8)
  - Rural Housing Service (RHS) Section 515/8
  - Loan Management Set-Aside (LMSA)
  - Property Disposition Set-Aside (PDSA)
  - Rental Assistance Demonstration Project-based Rental Assistance (RAD/PBRA)

11

11

Applicable Programs

- Other programs:
  - Section 202 Senior Preservation Rental Assistance Contracts (SPRAC)
  - Section 202/162 Project Assistance Contract (PAC)
  - Section 202 Project Rental Assistance Contract (PRAC)
  - Section 811 PRAC
  - Rent Supplement
  - Section 236 (including RAP)
  - Section 221(d)(3)/(d)(5) Below-Market Interest Rate (BMIR)

12

12

Does Not Apply To

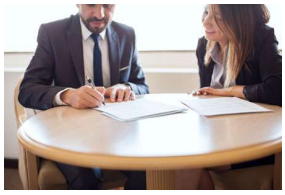
- Unassisted properties with a Section 221(d)(4) mortgage
- HOME
- Public and Indian Housing (PIH) programs
  - HCV, PBV, and public housing

13

13

Applicability

- Applies to applicants, assisted tenants, and industry partners working with these programs



14

14

Impacted Documents

- Pertains to all HUD forms and O/A-created documents related to:
  - Asset management
  - Section 8 contract renewals
  - Occupancy policies

15

15

Impacted Documents

- Types of forms and documents other than official HUD forms include, but are not limited to:
  - Documents transmitted among O/A, HUD, CA, and other service providers
  - Documents submitted by and provided to applicants or tenants
  - Documents submitted to and from third-party verifiers to O/A
  - Documents used for other HUD Multifamily Housing business purposes

16

16

Impacted Documents

- While not required by HUD, some state and local laws or entities may require the use of wet signatures on some forms
  - HUD-50059, "Owner's Certification of Compliance with HUD's Tenant Eligibility and Rent Procedures"
  - HUD-9887 "Document Package for Applicant's/Tenant's Consent"
  - Leases and lease addenda

17

17

Impacted Documents

- O/A are urged to consult with their legal counsel and obtain necessary information about state and local requirements for these types of documents

18

18

Definitions

19

19

Signatures

Digitized Signature

- Digital image of a handwritten signature
  - Sometimes used as an e-signature
- Scanned image of an ink-based signature handwritten on paper
- Image can be created by the signer using a digital pen and pad, or stylus to write his or her name in a manner that is captured and stored digitally

Digital Signature

- Encrypted data produced by a mathematical process applied to a record
- Includes a certificate of authority to ensure the validity of the person signing
- Sometimes used to authenticate a person or device and verify the integrity of the record

20

20

Electronic Signature

- An electronic sound, symbol, or process associated with a contract or record and executed by a person with the intent to sign the record
  - Typed names, a digital signature, digitized images of a handwritten name, Personal Identification Numbers (PIN), or just clicking an "I agree" button on a website

21

21

Wet Signature

- Created when a person physically marks a document
- "Wet" implies signature requires time to dry, as it was written in ink
- HUD's guidance refers to this as an "original signature"

22

22

Signatures

- Whether electronic or wet, a signature is the means by which a person indicates an intent to associate themselves with a document in a manner that has legal significance
- Constitutes legally binding evidence of the signer's intent regarding a document

23

23

E-signature Requirements

24

24

E-signature Requirements

- Notice sets forth for a signing process related to:
  - Electronic form of signature
  - Intent to sign
  - Association of signature to the record
  - Identification and authentication of the signer
  - Integrity of the signed record

25

25

Electronic Form of Signatures

26

26

Common E-signatures

- Variety of options available for e-signature
  - A typed name → Like at the end of an email
  - A digital image of a handwritten signature that is attached to an electronic record
  - A shared secret (password or PIN) used to sign the electronic record
    - Secret is known to the user and the system
  - A biometrics-based identifier → Fingerprint, voice print, or retinal scan

27

27

Common E-signatures

- Digital signature
- A sound recording of a person expressing consent
- Processes like using a mouse to click an "I Agree" button
- Using a private key and applicable software to apply a digital signature or scanning and applying a fingerprint

28

28

Intent to Sign

29

29

Intent to Sign

- *Intent* is determined by what a signer would have reasonably believed under the circumstances when the e-signature was applied
  - Assuming that person was not being coerced

30

30

Examples of Intent to Sign

- "By signing below, I agree to the foregoing contract terms"
- "By checking this box, I agree to the terms of use"
- "Click to agree"
- "By signing below, I attest that the information provided is true and agree to allow the O/A or HUD to verify such information"
- "I hereby certify that…"

31

31

Association of Signature to the Record

32

32

Association of Signature to the Record

- In order to be legally significant, the signature must be attached to or logically associated with the record being signed

33

33

Association of Signature to the Record

- *Association* means:
  - Must be clear to signer what they are signing
  - Signer must have an opportunity to review the record before signing it and to clearly understand the parameters of the record
  - The electronic form of the signature applied by the signer must be linked to the record being signed

34

34

Association of Signature to the Record

- Association must be done in a way that allows someone to later determine the record has been signed
  - The data constituting the e-signature must be stored so that it is permanently linked to or associated with the record that was signed

35

35

Identification and Authentication of the Signer

36

36

Identification and Authentication of the Signer

- If it is ever necessary to prove the validity of an e-signature in court, it will be necessary to prove who signed
  - Meeting this burden of proof requires establishing a link between an identified person and the signature

37

37

Identification and Authentication of the Signer

- Laws do not require the use of any particular method to identify or authenticate a party if the method used meets the requirement that it is as reliable as needed for the purpose in question
- It does not need to be part of the same process used to indicate the signer's intent if the person's identity and intent can be reliably correlated to the record signed

38

38

Integrity of the Signed Record

39

39

Integrity of the Signed Record

- O/As using e-signatures must ensure that documents signed electronically can't be altered after signing

40

40

Integrity of the Signed Record

- If changes are made, the electronic process must provide an audit trail showing:
  - All alterations
  - The date and time they were made
  - Who made them

41

41

Requirements for Systems with Digital Signatures

- A digital signature is a way to ensure that an electronic document or record is authentic
  - Any computer system or application that uses a username and password or multi-factor authentication contains digital signatures

42

42

Requirements for Systems with Digital Signatures

- *Authentic* means that you know:
  - Who created the document
  - It has not been altered in any way since that person created it
- A username and password are the most common form of authentication

43

43

44

44

Electronic Transmission of O/A Documents

- O/A may electronically transmit HUD-approved or required documents when local, state, or federal law permits
  - Does not apply to documents required by lenders, other government agencies, or private concerns

45

45

Documents sent to HUD or CA

- HUD and its CA may offer certain electronic transmission methods for documents
  - O/A should contact HUD field office or CA to determine each agency's submission options and/or transmission preferences

46

46

Documents Sent to O/A

- HUD and CA staff may electronically transmit HUD forms and documents to O/A or to each other as state, local, or federal laws permit
  - Adequate security measures and choice of transmission method must ensure the security of sensitive information included in such documents

47

47

Applicants and Tenants → O/A

- If an O/A chooses to use electronic communication, applicants and tenants may also choose to communicate electronically with the O/A

48

48

Applicants and Tenants → O/A

- May complete documents online or by hand and then transmit or scan and email them
- May submit information and documents using online systems, tablet or smartphone apps, email, or other electronic media
- O/A may designate specific methods as acceptable for electronic transmission

49

49

Applicants and Tenants → O/A

- Must have the opportunity to provide information and documents in paper copy
  - Including both before and after they have provided any information electronically or after they have done so and wish to discontinue

50

50

O/A → Applicants and Tenants

- O/A may provide documents and notices electronically or make such documents available in an electronic format
  - When state and local laws permit
- If an O/A chooses to provide documents electronically, the O/A should inform applicants or tenants of their option to receive documents in paper form

51

51

O/A → Applicants and Tenants

- If required forms, notices, and brochures are transmitted electronically, HUD recommends the O/A request an electronic acknowledgment of receipt
  - Where HUD does not require an acknowledgment, the O/A should still maintain records showing they provided the applicant/tenant with the information

52

52

O/A → Applicants and Tenants

- When local, state, federal laws, or HUD regulations require that specific documents be provided by first class mail, delivered in person, or other specified means, document must be provided using the required procedures and not solely transmitted electronically

53

53

Transmission Methods

54

54

Transmission Methods

- When transmitting documents electronically, industry partners must use National Institute of Standards and Technology (NIST) compliant methods
  - Putting the documents inside an encrypted wrapper, such as a password protected DOC, PDF, or ZIP file
- Passwords should not be included in the same transmission as the documents
- Best practice is to provide the recipient with the password by calling, texting, or in a separate email

55

55

Transmission Methods

- HUD strongly recommends using an encrypted transfer mechanism such as:
  - A shared link with an encrypted cloud storage service
  - An encrypted mail service
  - Web encrypted transfer tools

56

56

EIV

- EIV data stored electronically must be in a restricted access directory
  - If placed on portable media, labeled appropriately and encrypted using a NIST Compliant Cryptographic Module
- All emails containing EIV data must be encrypted using a NIST compliant cryptographic module- *no change here*

57

57

Transmission Methods

- Other methods for transmitting data must meet HUD's security requirements
  - Removable media, like a thumb drive or SD card
  - Direct access, like providing login information to a system where documents can be accessed
  - Other compliant technology as developed

58

58

Personally Identifiable Information

(PII)

59

59

What is PII?

- Information that can be used to trace a person's identity, either alone or when combined with other information that is linked to that individual
- Some examples include name, DOB, email address, medical history, birth certificate, or driver's license

60

60

PII

- All documents containing PII must be encrypted or transmitted in a secure manner

61

61

Faxing

- Use date stamp, verify intended recipient is available, then confirm recipient received the fax
  - Ensure none of the information is stored in the fax machine's memory
  - If possible, use a machine with a secure line

62

62

Email or Unsecured Information System

- Ensure the information and all attachments are encrypted
- Do not place PII on shared drives, multi-access calendars, intranet, or the internet unless they are NIST compliant
- Do not let documents with PII sit on a printer, scanner, or fax machine where unauthorized individuals can access the information

63

63

Privacy Act Violations

- The Privacy Act specifically provides civil remedies, including damages, and criminal penalties for violations of the Act
  - Criminal violations are limited to misdemeanors
  - May be fined up to $5,000 for violation

64

64

Electronic Storage

65

65

File and Document Storage

66

66

File and Document Storage

- HUD forms and O/A-created forms or documents may be electronically stored when state and local laws permit.
- O/As may:
  - Maintain paper files, electronic files, or a combination of both
  - Convert paper files to electronic format

67

67

File and Document Storage

- O/As are encouraged to consult legal counsel to determine when wet signatures are required by other federal, state, or local laws and/or agencies
- All information stored electronically must be encrypted using a NIST compliant encryption solution

68

68

Access

69

69

Access

- Industry professionals will access documents as required by the function of those documents
  - Maintenance will not have access to tenant certification records,
  - REAC inspectors will not have access to tenant files, etc.

70

70

Access

- Access to electronic information must comply with the same requirements paper files
  - O/As must ensure they are secure
  - Access to e-storage systems must be restricted to certain users based on specific HUD program guidance

71

71

Access

- Industry partners must comply with special rules surrounding EIV or other documents, such as a tenant or applicant's VAWA status

72

72

Stored Information

- Only used for it's intended purpose
- Will not be shared except by appropriate request
- Proprietary information will not be shared with another entity
  - A CA would not share one O/As rent comp study with another O/A

73

73

IPA

- Independent Public Auditors (IPA) have access to O/A electronic records while conducting HUD financial audits

74

74

75

75

Security

76

76

Security

- To ensure appropriate security, industry partners must comply with any specific data security requirements of HUD programs

77

77

Examples

- Encryption both at transmission and rest;
- Use and disclosure of data;
- Passwords for all employees, agents or contractors;
- Using and accessing electronic data and systems, backing up data, and data protection;
- Use of emails, message content, encryption, and file retention;
- Mobile devices - ensure they are secure, used appropriately, and protected from theft;
- Unauthorized access;
- Reporting malicious malware in the event it is inadvertently imported;
- Audit and access logs; and
- Data destruction

78

78

Security

- Report any breach to the integrity of any electronic data that contains either sensitive information or information pertaining to electronic signatures to the entity that owns or administers the data.
  - Should comply with federal, state or local laws, regulations, and guidance

79

79

Security

- Use a method to track electronic activity associated with sensitive documents and information
  - Have a method to disclose any data breach to those affected
  - Tracking methods should be designed to allow audits when requested by federal or state agencies
  - Audits must be conducted within the protections of the Privacy Act and other laws and regulations

80

80

Retention

81

81

Retention

- O/As should have a document or records retention policy to establish a protocol for retaining electronic data information for compliance needs
  - O/As must comply with program-specific document retention requirements
  - Retention requirements are the same for paper and electronic documents and records

82

82

Data and File Destruction

83

83

Data and File Destruction

- Data destruction is the process of destroying electronic data stored on electronic media, so that it is completely unreadable and cannot be accessed or used for unauthorized purposes
- Industry partners must have policies and procedures in place to destroy records and data and must document when and how records and data are destroyed

84

84

Data and File Destruction

- For paper files:
  - O/A must dispose of paper files in a manner that will prevent any unauthorized access to personal information, e.g., burn, pulverize, shred, etc.
  - When converting paper files/documents to electronic format, prior to destroying the paper, O/A must check local and state laws to determine if hard-copies with wet signatures must be retained or whether a print-out of an electronic document with a verifiable electronic signature is acceptable

85

85

HUD Review Impact

- Reviews conducted by HUD or CA in compliance with HUD's guidelines may involve reading files electronically (when available)
  - The files must be provided in compliance with HUD's or other federal/state/local government security access requirements
  - O/A may continue to furnish documents in paper format if they prefer

86

86

Regulatory Restrictions

87

87

Regulatory Restrictions Notices

- Some regulations require some notices to tenants be sent by first class mail, delivered directly to tenants or their units, or posted in public spaces
- In these situations, electronic communication does not satisfy the requirement
  - Email, posting on website, etc.
- *Notice lists some examples of notices*

88

88

Storage of Tenant Notices

- When the tenant is provided a notice in paper form, if O/A maintains electronic tenant files, they must scan and store an electronic file of the tenant notification in the tenant's file

89

89

Accessibility of Electronic Media

90

90

Accessibility of Electronic Media

- Industry partners must provide all notices and communications consistent with Section 504 and the ADA and its implementing regulations

91

91

Accessibility of Electronic Media

- These statutes also require effective communication with individuals with disabilities and prohibit Electronic and Information Technology (EIT) imposed barriers to accessing information, programs, and activities by persons with disabilities

92

92

Accessibility of Electronic Media

- O/As must provide appropriate auxiliary aids and services necessary to ensure effective communication, which includes ensuring that information is provided in appropriate accessible formats as needed
  - Or in another language for persons with Limited English Proficiency (LEP)

93

93

Accessibility of Electronic Media

- If a person with a disability is unable to use an electronic system or file that meets federal accessibility standards, O/A must provide reasonable accommodations to afford users an equal opportunity to participate
  - Completing and signing documents or submitting documents in paper copy

94

94

Final thoughts

- Still some questions to be answered by HUD
- Need to be thoughtful about any conversion activities
- MUST still offer paper process to residents/applicants

95

95

Questions?

Heather Sievers
hsievers@nanmckay.com
208-288-1104

Thank you for your time today

96

96