



ASSISTANT SECRETARY FOR HOUSING-
FEDERAL HOUSING COMMISSIONER

U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-8000

Special Attention of:

MF Regional and Satellite Directors
MF Asset Management Division Directors
Rural Services (RHS) Directors
Contract Administrators
MF Owners and Management Agents

Notice: H 2020-10

Issued: 11/6/2020

Expires: This notice remains in effect
until amended, revoked, or
superseded.

Subject: Electronic Signature, Transmission and Storage - Guidance for Multifamily Assisted
Housing Industry Partners

Contents:

- I. Purpose.
- II. Applicability.
- III. Background.
- IV. Definitions.
- V. Electronic Signature.
- VI. Electronic Transmission.
- VII. Electronic Storage.
- VIII. Regulatory Restrictions.
- IX. Accessibility of Electronic Media.
- X. Paperwork Reduction Act.
- XI. Contact Information.

I. Purpose.

This Notice 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) in the Office of Multifamily Housing Programs. For purposes of this Notice, "industry partners" include:

- Owners of HUD multifamily assisted housing properties;
- Management agents and service providers, and
- HUD and Contract Administrator (CA) staff.

With the issuance of this Notice, OAMPO permits, but does not require, industry partners to use electronic signatures. The Notice also permits industry partners to electronically transmit and electronically store files. Industry partners choosing to use electronic signatures, electronic transmission, and/or storage of electronic documents must do so in compliance with federal, state, and local laws.

Owners and management agents (O/A) adopting the terms of this Notice must provide applicants and tenants the option to utilize wet (i.e. original) signatures and paper documents upon request. When feasible, industry partners, applicants, and tenants should have the option of providing signatures and documents in wet or paper form.

This Notice does not change the nature or use of required documents as all such guidance remains the same. For example, an O/A may accept a tenant's notarized statement or signed affidavit regarding the veracity of information submitted, if the information cannot be verified by another acceptable verification method. However, the document may be submitted in paper form or signed and/or transmitted to the O/A electronically.

Except for the regulatory requirements (listed in Section VIII of this Notice), references to original signatures, original documents, the transmission or submission of documents, and file maintenance in established HUD assisted housing guidance may be interpreted and implemented through electronic means. Note that in the case of wet (i.e. original) signatures, the acceptable electronic equivalent must meet the criteria set forth in Section V of this Notice. Section VIII provides the regulatory requirements for wet signatures and use of paper documents. These requirements supersede the guidance in this program Notice and must be followed.

The contents of this document, except when based on statutory or regulatory authority or law, do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies

II. Applicability.

A. Multifamily Housing Programs.

This Notice is applicable to the following assisted multifamily housing programs and pertains to all applicants, assisted tenants, and industry partners working with these programs:

- Project-based Section 8 programs under the United States Housing Act of 1937 (42 U.S.C. 1437) as follows:
 - 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); and
 - Rental Assistance Demonstration Project-based Rental Assistance (RAD/PBRA).
- 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 and Project Rental Assistance (PRA);
 - Rent Supplement;
 - Section 236 (including RAP); and
 - Section 221(d)(3)/(d)(5) Below-Market Interest Rate (BMIR).

The guidance in this Notice does not apply to unassisted properties with a Section 221(d)(4) mortgage, the HOME program, or to Public and Indian Housing (PIH) programs.

If guidance is provided by another federal or state agency, such direction may not circumvent the guidance provided in this Notice when the property is operating under any of the eligible programs listed above. If there is conflicting guidance, O/A should refer to HUD Handbook 4350.3, REV-1, Occupancy Requirements of Subsidized Multifamily Housing Programs, Chapter 1, for further information.

B. Impacted Documents.

This Notice pertains to all HUD forms and O/A created documents related to OAMPO's asset management, Section 8 contract renewal, and occupancy policies. Any such forms and documents that comply with HUD guidelines may be signed, transmitted, and stored electronically. Types of forms and documents other than official HUD forms include, but are not limited to, the following:

- 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; and
- Documents used for other HUD Multifamily Housing business purposes.

Note that, while not required by HUD, some state and local laws or entities may require the use of wet signatures on some forms, such as:

- 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" and
- Leases and lease addenda.

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

III. Background.

The use of electronic signatures in transactions involving federal organizations is primarily governed by one or more of the following laws (“E-Transaction Laws”):^{1 2}

- A. [Electronic Signatures in Global and National Commerce Act](#) (E-SIGN) (15 U.S.C. § 7001 et. seq., effective October 1, 2000). E-SIGN promotes the use of electronic contract formation, signatures, and recordkeeping in private commerce by establishing legal equivalence between contracts written on paper and contracts in electronic form, pen-and-ink signatures and electronic signatures, and other legally required written documents and the same information in electronic form.

E-SIGN supersedes all statutes or federal agency rules containing paper-based requirements that might otherwise discourage the use of electronic signatures and records in consumer, commercial, or business transactions between two or more private parties.

In such situations, all contracting parties agree to the use of electronic methods. E-SIGN generally preserves an agency’s existing authority to specify standards and formats for records filed with the agency E-SIGN, Section 104(a)).

- B. [The Uniform Electronic Transactions Act](#) (UETA), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999 and has been adopted by 47 states, the District of Columbia, and the U.S. Virgin Islands as of November 2010. The three states that have not adopted the UETA (New York, Illinois, and Washington) have all adopted similar laws making electronic signatures legally enforceable. UETA provides that when a law requires either a record to be in writing or include a signature, an electronic record or an electronic signature can satisfy that requirement, so long as the parties to the transaction have agreed to proceed electronically.
- C. Government Paperwork Elimination Act (GPEA) (44 U.S.C. § 3504, enacted in 1998) applies to governmental transactions and other transactions involving certain federal organizations. GPEA requires Federal agencies to allow individuals or entities that deal with those agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. The Act specifically states that electronic records and their related

¹Appendix II to OMB Circular A-130, Implementation of the Government Paperwork Elimination Act, November 2000, available at https://obamawhitehouse.archives.gov/omb/circulars_a130_a130appendix_ii

² “Use of Electronic Signatures in Federal Organization Transactions”, January 25, 2013 , Federal CIO Council <https://docplayer.net/6709446-Use-of-electronic-signatures-in-federal-organization-transactions-version-1-0-january-25-2013.html>.

electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form and encourages Federal government use of a range of electronic signature alternatives.³

IV. Definitions.

- A. Digital signatures are encrypted data produced by a mathematical process applied to a record using a hash algorithm and public key cryptography. Digital signatures are considered the most “secure” type of electronic signature. They include a certificate of authority to ensure the validity of the signatory (the signature’s author and owner). Digital signatures are sometimes used as an electronic signature, as part of a process to authenticate a person or device, and to verify the integrity of the record.^{4 5}

Digitized Signature is a digital image of a handwritten signature. The image can be as simple as a scanned image of an ink-based signature handwritten on paper. In some cases, the image is created by the signer using a special computer input device, such as a digital pen and pad, to write out his or her name in a manner that is captured and stored digitally. A digital image of a handwritten signature is sometimes used as an electronic signature.⁶

- B. Electronic Record means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.⁷
- C. Electronic signature means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. In a paper environment, a common form of signature is one’s handwritten name. In an electronic environment, commonly used forms of signature include typed names, digitized images of one’s handwritten name,

³ The Office of Management and Budget’s (OMB) Implementation of the Government Paperwork Elimination Act https://obamawhitehouse.archives.gov/omb/fedreg_gpea2/

⁴ “Use of Electronic Signatures in Federal Organization Transactions”, January 25, 2013 , Federal CIO Council <https://docplayer.net/6709446-Use-of-electronic-signatures-in-federal-organization-transactions-version-1-0-january-25-2013.html>

⁵ Electronic Signatures in Global and National Commerce Act (E-SIGN) (15 U.S.C. § 7001 et. seq., effective October 1, 2000) <https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter96&edition=prelim>

⁶ “Use of Electronic Signatures in Federal Organization Transactions”, January 25, 2013 , Federal CIO Council <https://docplayer.net/6709446-Use-of-electronic-signatures-in-federal-organization-transactions-version-1-0-january-25-2013.html>

⁷ Electronic Signatures in Global and National Commerce Act (E-SIGN)(15 U.S.C. § 7001 et. seq., effective October 1, 2000) <https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter96&edition=prelim>

Personal Identification Numbers (PIN), clicking an “I Agree” button on a website, or a digital signature.⁸

- D. Personally Identifiable Information (PII) “refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.... To determine whether information is PII, [an] agency shall perform an assessment of specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual.” Some examples of PII include name, date of birth (DOB), email address, mailing address, medical history, family relationships, vehicle identifiers including license plates, unique names, birth certificate, license, telephone and/or other specific reference numbers and/or any information that can directly identify an individual.⁹
- E. Record means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.¹⁰
- F. Sensitive Personally Identifiable Information (sensitive PII) is a higher risk subset of PII. Sensitive PII is PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Such general data as social security numbers, bank account, or passport information, credit and/or debit card numbers, driver’s license numbers, and healthcare or medical insurance related information is considered sensitive PII.¹¹
- G. Signature, whether electronic or on paper (“wet”), is the means by which a person indicates an intent to associate himself/herself with a document in a manner that has legal significance. It constitutes legally binding evidence of the signer’s intention regarding a document.¹²

⁸ “Use of Electronic Signatures in Federal Organization Transactions”, January 25, 2013 , Federal CIO Council <https://docplayer.net/6709446-Use-of-electronic-signatures-in-federal-organization-transactions-version-1-0-january-25-2013.html>

⁹ Office of Management and Budget (OMB) Memorandum-17-12, “Preparing for and Responding to a Breach of Personally Identifiable Information”, January 3, 2017 www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-17-12.pdf

¹⁰ Electronic Signatures in Global and National Commerce Act (E-SIGN)(15 U.S.C. § 7001 et. seq., effective October 1, 2000) <https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter96&edition=prelim>

¹¹ HUD Breach Notification Response Team (HBNRT) Privacy Breach Standard Operating Procedures, Section 3.3, <https://www.hud.gov/sites/documents/31502cioh.pdf>

¹² “Use of Electronic Signatures in Federal Organization Transactions”, January 25, 2013 , Federal CIO Council <https://docplayer.net/6709446-Use-of-electronic-signatures-in-federal-organization-transactions-version-1-0-january-25-2013.html>

H. Wet signatures are created when a person physically marks a document. In some cultures, this is done by writing a name in a stylized, cursive format (or even a simple “X”) on a piece of paper. The word “wet” implies that the signature requires time to dry, as it was made with ink.¹³ (Much of HUD’s policy guidance refers to “original signatures”, which have the same meaning as wet signatures.)

V. Electronic Signatures.

A. Introduction.

Much of the information in this Section V is taken directly from “[Use of Electronic Signatures in Federal Organization Transactions](#)”, guidance issued by the Federal Chief Information Officer (CIO) Council in January 2013. Industry partners are encouraged to download and review this document along with this program Notice. It provides greater discussion and detail on the items discussed in this Section.

The E-Transaction Laws, (see Section III of this Notice), essentially answers the basic question “if the law requires a ‘signature’, how can an electronic transaction satisfy that requirement”? This is done by what is referred to as the “functional equivalence approach”. This approach considers the purposes and functions of the traditional paper-based requirement for a signature and specifies how those purposes or functions can be fulfilled in an electronic context. This section sets forth the following requirements for a signing process that will satisfy requirements and guidance in all three E-Transaction Laws:

- Electronic form of signature;
- Intent to sign;
- Association of signature to the record;
- Identification and authentication of the signer; and
- Integrity of the signed record.

The “technology neutrality” principle holds that the law should not discriminate among different forms of technology, provided that they meet the five requirements listed above.

B. Electronic Form of Signature.

In a paper-based transaction, the most used form of signature is a person’s name, written with ink and in his or her own handwriting (i.e., a wet signature). To comply with requirements set forth in the Fair Housing Amendments Act and Section 504 of the Rehabilitation Act, entities may also be required to accept alternative methods (e.g., signature stamps) as a reasonable accommodation.

[2013.html](#).

¹³ “The Difference Between Wet, Digital & Electronic Signatures” <https://www.laserfiche.com/ecmblog/whats-the-difference-between-wet-digital-and-electronic-signatures/>

The E-Transaction laws similarly recognize that electronic signatures can take many forms and can be created by many different technologies, as long as the signing process satisfies the other requirements identified above and further described below. Examples of commonly used electronic forms of signature include:

1. Symbols such as:

- A typed name (e.g., 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 shared secret (e.g., a secret code, password, or PIN) used by a person to sign the electronic record. (“Shared” means that the secret is known both to the user and to the system);
- A unique biometrics-based identifier (e.g., a fingerprint, voice print or a retinal scan); or
- A digital signature.

2. Sounds such as:

- A sound recording of a person’s voice expressing consent;
- Processes such as using a mouse to click a button (such as clicking an “I Agree” button); and
- Using a private key and applicable software to apply a “digital signature” or scanning and applying a fingerprint.

This is not an exhaustive list, but it illustrates the variety of options available for use as an electronic form of signature. As technology advances, future methods may be adopted.

C. Intent to Sign.

In electronic transactions, merely applying a person’s name, a digital signature, or any other sound, symbol, or process to an electronic record does not necessarily qualify it as a legally binding signature. For an electronic form of signature to be legally effective as an electronic signature, it must be executed or adopted by the signer with an intent to sign. Intent is the critical component of any legally binding signature. The existence of intent to sign is determined by what a signer would have reasonably believed under the circumstances when the electronic form of signature was applied, assuming that he or she was not being coerced. Designing a signature process that establishes the intent to sign can be done through a variety of methods that provide a clear and conspicuous indication that a signature is being created and that it will be legally binding. It is important that the record, and/or process by which a person applies an electronic form of signature to the record, be designed to indicate the means by which the signer can indicate his or her intent to sign the record.

Following are some examples:

- “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”, and
- “I hereby certify that...”.

D. Association of Signature to the Record.

In a paper-based transaction, a document is typically signed by writing one’s name directly on the document to be signed. Writing one’s name on a blank sheet of paper, for example, will not qualify as a signature for any specific document. By its very nature, signing a document requires putting the signature directly on the document. The same requirement is carried over to electronic records.

The E-Transaction laws require that the electronic form of signature be made a part of the record being signed. Specifically, in order to be legally significant, the signature must be attached to or logically associated with the record being signed. “Association” means:

- The process must be clear to the signer as to exactly what it is that he or she is signing;
- The signer must have an opportunity to review the record before signing it and to clearly understand the parameters of the record he or she is signing; and
- The electronic form of the signature applied by the signer must be linked to the record being signed.

The association must be done in a manner that allows someone to later determine that the record has been signed. The data constituting the electronic form of signature must be stored in a way that permanently associates it with the electronic record that was signed.

E. Identification and Authentication of the Signer.

By definition, a signature must be the act of a specific signer. If the alleged signer denies signing, the signature will usually be unenforceable, unless there is proof that the alleged signer did sign. If it is ever necessary to prove the validity of an electronic 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.

While authentication of the signer’s identity is an important part of the signing process, it may or may not be the electronic form of signature that provides proof of identity. As long as the overall signing process addresses identity and authentication, it is acceptable.

The E-Transaction laws do not require the use of any method to identify or authenticate a party as long as the method selected satisfies the requirement that it be as reliable as appropriate for the purpose in question. It does not need to be part of the same step or process that indicates the signer’s intent as long as the person’s identity and intent can be

reliably correlated to the record he or she is signing.

F. Integrity of the Signed Record.

The usability, admissibility, and provability of a signed electronic record requires that procedures be undertaken to ensure the continuing integrity of both the electronic record and its electronic signature, following completion of the signing process. It is a matter of providing appropriate data security for both the record and the signature.

Data integrity is concerned with the accuracy and completeness of electronic information communicated over the Internet or stored in an electronic system. Data integrity ensures that no unauthorized alterations are made to such information either intentionally or accidentally. Ensuring integrity requires guarding against information modification or destruction for the full retention period of the record.

Industry partners utilizing e-signatures must ensure that documents signed electronically cannot be altered. If changes to the document are made, the electronic process must be designed to provide an “audit trail”, showing all alterations, the date and time they were made, and the identity of the person who made them.

G. Requirements for Systems with Digital Signatures.

As explained above in Section IV.A, a digital signature varies from other electronic forms of signature, as it is “Encrypted data produced by a mathematical process applied to a record using a hash algorithm and public key cryptography”. Any computer system or application that uses a username and password or multi-factor authentication would contain digital signatures. A digital signature is a way to ensure that an electronic document or record is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it. A username and password are the most common form of authentication.

In their work with HUD programs, many industry partners likely use computer systems or applications that contain digital signatures. For these digital signatures to be considered a legal form of electronic signature, the system or application must conform to the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Digital Signature Standard 186-4 and other Federal Government digital signature regulations and guidance. Compliant software programs will contain a security feature that ensures that the digital signature is unique and protected and that only the “owner” of the signature maintains control of its use.^{14 15}

¹⁴ “Use of Electronic Signatures in Federal Organization Transactions”, January 25, 2013 , Federal CIO Council <https://docplayer.net/6709446-Use-of-electronic-signatures-in-federal-organization-transactions-version-1-0-january-25-2013.html>

¹⁵ National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) [Digital Signature Standard 186-4](https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf), <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf>

VI. Electronic Transmission.

A. Owner/Agent Documents.

This Notice permits electronic transmission of HUD-approved or required documents when local, state, or federal law permits. It does not provide guidance on documents required by lenders, state or local government agencies, or other private concerns.

Note: Relevant program files or information can be transferred in a format that is acceptable to both parties, whether that is electronic or paper.

1. Documents Sent to HUD or a CA.

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

2. 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. As noted above, adequate security measures and choice of transmission method must ensure the security of sensitive information included in such documents.

B. Applicants and Tenants.

1. Submission to O/A.

If an O/A chooses to utilize electronic communication procedures, Applicants and tenants may also choose to communicate electronically with the O/A. Their choice must be made affirmatively (not assumed with an opt-out procedure). (See E-SIGN Act, 15 U.S.C. 7001(c)(1)(A)). They may complete most documents online or by hand and then transmit and/or scan and email them electronically to an O/A.

Applicants and tenants may also submit information and documents using other methods, such as online systems, tablet or smart phone apps, email, or other electronic media. O/A may designate specific methods as acceptable for electronic transmission. However, applicants and tenants must have the opportunity (if they desire) to provide information and documents in paper copy, including both before they have provided any information or documents electronically or after they have done so and wish to discontinue.

2. Transmission to 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 such documents in paper form.

If required notices, forms, and brochures are distributed electronically, HUD recommends that O/A request an electronic acknowledgement of receipt. Where HUD does not specifically require applicant or tenant acknowledgement of

receipt, O/A should nonetheless maintain records showing that they provided applicants or tenants with the electronic file or the electronic address used to access the document.

When providing documents, forms, or notices electronically, O/A must be sure to comply with tenant notification requirements in Handbook 4350.3, HUD program Notices, and state and local laws, and regulations. When local, state, federal laws or regulations require that specific documents be provided by first class mail, delivered in person, or other specified means, this document must be provided using the stated required procedures and may not be solely transmitted electronically. (Refer to Section VIII of this Notice.)

C. Transmission Methods.

1. When transmitting documents electronically, industry partners must use National Institute of Standards and Technology (NIST) compliant methods. Examples include 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. It is preferable to provide the recipient with the password by calling, texting, or in a separate email. HUD strongly recommends using an encrypted transfer mechanism such as a shared link with an encrypted cloud storage service, an encrypted mail service, or web encrypted transfer tools.
2. When transmitting and storing Enterprise Income Verification (EIV) system data, vendors must adhere to NIST compliant standards. Handbook 4350.3 REV-1, Chapter 9-21(C)(1)(a)). EIV data stored electronically must be in a restricted access directory or, if placed on portable media, labeled appropriately and encrypted using a [NIST Compliant Cryptographic Module](#). Similarly, all emails containing EIV data must be encrypted using a NIST compliant cryptographic module.
3. Other possible methods for transmitting electronic documents and data must comply with HUD's security requirements. They may include but are not limited to the following:
 - a. Removable electronic media, such as thumb drives or SD cards;
 - b. Direct access (i.e., providing login information to a system in order to access electronically signed and/or stored documents); and
 - c. Other compliant technology as developed.

D. Personally Identifiable Information (PII).

1. All documents containing or conveying PII must be encrypted or transmitted in a secure manner in order to safeguard this information.

- a. When faxing sensitive PII, use the date stamp function; confirm the fax number, verify that the intended recipient is available and confirm that he/she has received the fax. Ensure that none of the transmission is stored in memory on the fax machine, and that all paper waste is disposed of properly (shredded). If possible, use a fax machine that uses a secure transmission line.
 - b. If a secure line is not available, contact the recipient's office prior to faxing to inform them that information is coming. Next, contact the recipient's office following transmission to ensure they received it. For each event, the best course of action is to limit access of PII only to those individuals authorized to handle it and create a paper trail and verify that information reached its destination.
 - c. When sending sensitive PII via email or via an unsecured information system, make sure the information and any attachments are encrypted.
 - d. Do not place PII on shared drives, multi-access calendars, on Intranet, or the Internet unless they are compliant with the terms of this Notice, including Section VI.C.2.
 - e. Do not let documents with PII sit on a printer, scanner, or fax machine where unauthorized employees or contractors can have access to the information.
2. Privacy Act Violations.

The Privacy Act of 1974 (5 U.S.C. Sec. 552a(g) and (i)) specifically provides civil remedies, including damages, and criminal penalties for violations of the Act. In the case of criminal violations, the Privacy Act limits these penalties to misdemeanors. An officer or employee of an agency may be fined up to \$5,000 for, when "knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it," as may "[a]ny person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses."¹⁶

VII. Electronic Storage.

A. File and Document Storage.

HUD forms and O/A created forms or documents used for the management of the property may be stored electronically when state and local laws permit. If industry partners want to utilize e-storage policies, they may do the following:

- Maintain paper files, electronic files, or a combination of both; and

¹⁶ <https://www.justice.gov/opcl/criminal-penalties>

- Convert paper files to electronic format.

Note: O/A are strongly encouraged to consult their legal counsel in determining the requirements for wet signatures for documents required by other federal, state, or local laws and/or agencies. O/A must ensure they maintain documents in appropriate formats.

When information is stored electronically, data must be encrypted using a NIST compliant encryption solution.

B. Access.

1. Industry professionals will access documents as required by the function of those documents. (For example, maintenance staff will not have access to tenant certification records. Real Estate Assessment Center (REAC) inspectors will not have access to tenant files.)
2. Access to electronic information must comply with the same HUD program requirements that apply to paper files. Industry partners must ensure the security of important electronic records and documents. Access to e-storage systems must be restricted to certain users based on specific HUD program guidance.
3. Industry partners must adhere to special rules surrounding EIV or other documents, such as documents disclosing a tenant's/applicant's status as a victim of domestic violence, dating violence, sexual assault, or stalking.
4. Industry partners will use the stored information only for its intended purpose and must not share any electronic or paper files for purposes other than those strictly related to an appropriate request. Proprietary information must not be shared with another like entity. (For example, a CA would not share rent comparability studies submitted by one O/A with another O/A.)
5. This Notice permits Independent Public Auditors (IPA), while conducting HUD financial audits, to have access to O/A electronic records, with the exception of EIV data. As identified in the Rules of Behavior for Use of EIV Information (for Individuals Without Access to the EIV System), EIV data must only be viewed within hardcopy files and only in the offices of the O/A or CA. Disclosure of EIV data in any other form (including transmitting the data through secure electronic means) violates Section 453 of the Social Security Act and Multifamily Housing's Computer Matching Agreements.

C. Security.

Data and information stored electronically must be maintained and used in ways that ensure the security, protection, and confidentiality of any information as required by federal, state, or local law. Data security management is a way to maintain the

integrity of electronic data and to make sure that the electronic data are not accessible by unauthorized parties or susceptible to corruption.

To ensure appropriate security, industry partners must comply with the following practices:

1. Comply with any specific data security requirements of HUD programs, relating to such activities and media as the following:
 - Encryption both at transmission and at rest;
 - Use and disclosure of data;
 - Passwords for all employees or agents/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.
2. 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. Such security policies should comply with federal, state or local laws, regulations, and guidance.
3. Utilize a method to track electronic activity associated with sensitive documents and information. In the event of a data breach, industry partners should have a method to facilitate disclosure to those affected by the breach. Such tracking methods should also be designed in such a way as to allow security audits of the electronic data when requested by federal or state agencies. Such audits must be permissible and conducted within the protections of the Privacy Act and other privacy and confidentiality laws and regulations.

D. Retention.

A data retention policy, or records retention policy, is an organization's established protocol for retaining electronic data information for operational or regulatory compliance needs. Industry partners must comply with established program-specific document retention requirements. Refer to Multifamily Housing handbooks for record retention requirements. Retention requirements are the same for both paper and electronic documents and records. Additionally, like paper documents and records, electronically stored and/or signed documents and records must be kept within a document management system where access is limited based on function and need to know. This is also the case when records and documents are stored in a central

location using document management software and when a secured version of a form is attached to a specific tenant or O/A record.

E. Data and File Destruction.

Data destruction is the process of destroying electronic data stored on tapes, hard disks, and other forms of 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.

1. Electronic Data.

Industry partners must have policies and procedures in place to destroy electronic data and must document when and how records and data are destroyed. Procedures must ensure that records and documents cannot be accessed once they have been destroyed. The type of destruction method used should correlate to the sensitivity of the data and HUD's or other federal/state/local government requirements.

2. Paper File Destruction.

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 and prior to destroying the paper format, O/A must check local and state laws and practices to determine if hard-copy documents with wet signatures must be retained or whether a print-out of an electronic document with a verifiable electronic signature is acceptable.

F. HUD Review Impact.

Reviews conducted by HUD or HUD's agents or reviews conducted 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.

VIII. Regulatory Restrictions.

Sections of HUD's regulations for multifamily housing programs (found in 24 Code of Federal Regulations (CFR)) 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 (email, posting on a website, etc.) does not satisfy the requirement. O/A and industry partners must comply with current and future regulatory requirements. Regulatory requirements supersede the administrative requirements provided in this Notice and other HUD Multifamily Housing handbooks and notices.

A. These include but are not limited to the following types of Notices:

- Termination notice (§247.4(b));

- Change in leasing and/or occupancy requirements, e.g., proposed pet rules (§5.353(f)).
- Increase in Maximum Permissible Rents (Section 245.310);
- Conversion of a project from project-paid utilities to tenant-paid utilities, or a reduction in tenant utility allowances (§ 245.410);
- Conversion of residential units in a multifamily housing project to a nonresidential use or to condominiums, or the transfer of the project to a cooperative housing mortgagor corporation or association (§ 245.410);
- A partial release of mortgage security (except for any release of property from a mortgage lien with respect to a utility easement or a public taking of such property by condemnation or eminent domain) (§ 245.410); and
- Making major capital additions to the project. (The term “major capital additions” includes only those capital improvements that represent a substantial addition to the project. Upgrading or replacing existing capital components of the project does not constitute a major capital addition to the project.) (§ 245.410).

B. Storage of Tenant Notices.

If O/A maintain electronic tenant files, they must scan and store an electronic file of the tenant notification in the tenant’s file, when the tenant is provided a notice in paper form.

IX. Accessibility of Electronic Media.

- A. Industry partners must provide all notices and communications discussed in this Notice consistent with Section 504 of the 1973 Rehabilitation Act and HUD’s Section 504 regulations, and Titles II or III of the Americans with Disabilities Act (ADA) and its implementing regulations. 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.

Industry partners 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, e.g., Braille, audio, large type, assistive listening devices, sign language interpreters, accessible websites and other electronic communications. In the event that 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 (e.g., in completing and signing documents or submitting documents in paper copy). (See 24 CFR 8.6; 28 CFR 35.160, 36.303.)

- B. Section 508 of the 1973 Rehabilitation Act requires federal agencies to ensure, when developing, procuring, maintaining, or using EIT, that the EIT allows persons with disabilities to access and use information and data comparably to those without disabilities, unless an undue burden would result to the Federal agency. HUD encourages O/A to adopt the goals and objectives of Section 508 by ensuring comparable access whenever EIT is used.

C. In accordance with Executive Order 13166 (E.O. 13166), it is the responsibility of housing providers to ensure that effective communication of electronic media includes reasonable steps taken to ensure meaningful access for persons with Limited English Proficiency (LEP) across technological platforms. Such formats may include, but are not limited to, multilingual websites and other electronic media.

X. Paperwork Reduction Act.

The information collection requirements contained in this Notice have been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3520). In accordance with the Paperwork Reduction Act, HUD may not conduct or sponsor, and a person is not required to respond to, a collection of information unless the collection displays a currently valid OMB control number.

XI. Contact Information.

Questions concerning this Notice should be directed to your property's Account Executive in your local HUD MF Regional or Satellite Office. You may also contact Annecia Durr, Branch Chief, Assisted Housing Subsidy Oversight, Department of Housing and Urban Development, 451 Seventh Street, SW, Washington, DC 20410, Annecia.Durr@hud.gov. Persons with hearing or speech impairments may access their field office via TTY by calling the Federal Relay Service at (800) 877-8339 (www.gsa.gov/fedrelay).

Dana T. Wade
Assistant Secretary for Housing
– Federal Housing Commissioner