Memorandum

Date:	June 9, 2026
To:	Honorable Chairman Anthony Rodriguez and Members, Board of County Commissioners
From:	Daniella Levine Cava Mayor
Subject:	Resolution authorizing the County Mayor or County Mayor's Designee to execute Memorandum of Agreement (Agreement) between Miami Dade County through the Housing and Community Development Department (HCD) and the Miami Dade County Property Appraiser's Office (PAMDC) for the limited purpose of sharing Housing Choice Voucher (HCV) participant address and landlord information

HC
Agenda Item No. 3(D)

Executive Summary

On January 21, 2026, the Miami-Dade County Board of County Commissioners (Board) adopted Resolution No. R-38-26, which authorized the County Mayor or County Mayor's designee to execute a Memorandum of Agreement between Miami-Dade County, by and through its Housing and Community Development Department (HCD), and the Property Appraiser of Miami-Dade County (PAMDC) related to the sharing of certain information of tenants and landlords participating in the County's Section 8 Housing Choice Voucher program (HCV program).

Subsequent to the adoption of Resolution No. R-38-26, HCD and PAMDC had further discussions related to the agreement, which was approved by the Board. As a result of these discussions, HCD and PAMDC have agreed to make additional changes to the memorandum of agreement (Revised Agreement). The agreement has been updated to clarify and expand the categories of documents and information that HCD is required to provide to PAMDC. These revisions specify the required documentation, applicable timelines, and the format in which materials must be transmitted to ensure compliance and facilitate PAMDC's review and oversight responsibilities. The hold harmless and indemnification section has been revised to more clearly define the parties' respective responsibilities and liabilities. The updated provision delineates the scope of indemnification, clarifies the circumstances under which indemnity applies, and addresses limitations consistent with federal, state, and local requirements governing HCD's operations. The revised agreement now incorporates, as exhibits, the legal opinion issued by the United States Department of Housing and Urban Development's (HUD) Office of General Counsel and the relevant HUD directives. These documents provide authoritative guidance regarding program requirements and are included to ensure consistency with federal regulations and to document the regulatory framework applicable to the parties' obligations under the Agreement.

Recommendation

It is recommended that the Board amend Resolution No. R-38-26, to approve the terms of and authorize the County Mayor or County Mayor's designee to execute the Revised Agreement, and to exercise all provisions contained therein, including, but not limited to termination and amendment provisions that are consistent with the attached resolution and Resolution No. R-38-26.

Scope
This item seeks to authorize the County, through HCD to share certain information with PAMDC. This agenda item has a countywide impact.

Fiscal Impact/Funding Source
This item will have no fiscal impact to the County.

Track Record/Monitor
Victor Atkins, HCD Assistant Director, Housing Programs will be responsible for monitoring compliance with the Revised Agreement.

Delegation of Authority
Upon the approval of the resolution, the County Mayor or County Mayor's designee will be authorized to execute the Revised Agreement and exercise all provisions contained therein, including, but not limited to termination and amendment provisions.

Background
Property assessment relies in part on verifying the nature and occupancy status of residential rental properties within Miami-Dade County. HCD and PAMDC seek to collaborate through an "Agreement" that will allow HCD to share limited HCV program data—specifically participant addresses and landlord names—for property assessment and compliance purposes. The "Agreement" includes detailed provisions to safeguard all Personally Identifiable Information (PII) in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a), applicable Florida privacy laws, and County data-security protocols, including encryption, access control, and breach notification requirements. The exchange of such information between County departments is in the best interest of the County, supports accurate property valuation, and enhances interdepartmental coordination without compromising participant privacy. On January 21, 2026, the Board adopted Resolution No. R-38-26, which authorized the execution of a memorandum of agreement to facilitate the exchange of information between HCD and PAMDC. Subsequent to the adoption of Resolution No. R-38-26, HCD and PAMDC discussed further revisions to the agreement that would require the Board's approval. The agreement has been updated to clarify and expand the categories of documents and information that HCD is required to provide to PAMDC. These revisions specify the required documentation, applicable timelines, and the format in which materials must be transmitted to ensure compliance and facilitate PAMDC's review and oversight responsibilities. The hold harmless and indemnification section has been revised to more clearly define the parties' respective responsibilities and liabilities. The updated provision delineates the scope of indemnification, clarifies the circumstances under which indemnity applies, and addresses limitations consistent with federal, state, and local requirements governing HCD's operations. The Revised Agreement now incorporates, as exhibits, the legal opinion issued by the United States Department of Housing and Urban Development's Office of General Counsel and the relevant HUD directives. These documents provide authoritative guidance regarding program requirements and are included to ensure consistency with federal regulations and to document the regulatory framework applicable to the parties' obligations under the Agreement.

Jimmy Morales
Chief Operating Officer

MEMORANDUM

(Revised)

TO: Honorable Chairman Anthony Rodriguez
and Members, Board of County Commissioners

DATE: July 21, 2026

FROM: Geri Bonzon-Keenan
County Attorney

SUBJECT: Agenda Item No.

Please note any items checked.

_____ **"3-Day Rule" for committees applicable if raised**

_____ **6 weeks required between first reading and public hearing**

_____ **4 weeks notification to municipal officials required prior to public hearing**

_____ **Decreases revenues or increases expenditures without balancing budget**

_____ **Budget required**

_____ **Statement of fiscal impact required**

_____ **Statement of social equity required**

_____ **Ordinance creating a new board requires detailed County Mayor's report for public hearing**

_____ **No committee review**

_____ **Requires more than a majority vote (i.e., 2/3's present ____, 2/3 membership ____, 3/5's ____, unanimous ____, majority plus one ____, CDMP 7 votes (majority of membership) ____, CDMP 2/3 members present but not less than 7 votes (majority of membership) ____, CDMP 9 votes (2/3 membership) _____) to approve**

_____ **Current information regarding funding source, index code and available balance, and available capacity (if debt is contemplated) required**

Approved _____ Mayor Agenda Item No.
Veto _____
Override _____

RESOLUTION NO. _____

RESOLUTION AMENDING RESOLUTION NO. R-38-26, TO APPROVE THE TERMS OF AND AUTHORIZE THE COUNTY MAYOR OR COUNTY MAYOR'S DESIGNEE TO EXECUTE A REVISED MEMORANDUM OF AGREEMENT, AND TO EXERCISE ALL PROVISIONS CONTAINED THEREIN, INCLUDING, BUT NOT LIMITED TO TERMINATION AND AMENDMENT PROVISIONS

WHEREAS, this Board desires to accomplish the purposes outlined in the accompanying memorandum, a copy of which is incorporated herein by reference,

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF COUNTY COMMISSIONERS OF MIAMI-DADE COUNTY, FLORIDA, that:

Section 1. The matters contained in the foregoing recital and accompanying memorandum are incorporated in this resolution by reference.

Section 2. This Board amends Resolution No. R-38-26, to approve the terms of and authorize the County Mayor or County Mayor's designee to execute the revised memorandum of agreement, attached hereto as Attachment "A" and incorporated herein by reference, and to exercise all provisions contained therein, including, but not limited to termination and amendment provisions that are consistent with this resolution and Resolution No. R-38-26.

The foregoing resolution was offered by Commissioner , who moved its adoption. The motion was seconded by Commissioner and upon being put to a vote, the vote was as follows:

Anthony Rodriguez, Chairman
Kionne L. McGhee, Vice Chairman

Marleine Bastien	Juan Carlos Bermudez
Sen. René García	Oliver G. Gilbert, III
Roberto J. Gonzalez	Keon Hardemon
Danielle Cohen Higgins	Vicki L. Lopez
Natalie Milian Orbis	Raquel A. Regalado
Micky Steinberg	

The Chairperson thereupon declared this resolution duly passed and adopted this 21st day of July, 2026. This resolution shall become effective upon the earlier of (1) 10 days after the date of its adoption unless vetoed by the County Mayor, and if vetoed, shall become effective only upon an override by this Board, or (2) approval by the County Mayor of this resolution and the filing of this approval with the Clerk of the Board.

MIAMI-DADE COUNTY, FLORIDA
BY ITS BOARD OF
COUNTY COMMISSIONERS

JUAN FERNANDEZ-BARQUIN, CLERK

By:_____
Deputy Clerk

Approved by County Attorney as
to form and legal sufficiency.

Terrence A. Smith

MEMORANDUM OF AGREEMENT

BETWEEN
MIAMI-DADE COUNTY
AND
PROPERTY APPRAISER OF MIAMI-DADE COUNTY

I. PARTIES

This Memorandum of Agreement ("Agreement") is entered into by and between the Miami-Dade County, a political subdivision of the State of Florida, by and through its Housing and Community Development Department ("County" or "MDHCD"), located at 701 NW 1 Court, 16th Floor, Miami, Florida 33136, and the Property Appraiser of Miami-Dade County ("PAMDC"), located at 111 NW 1st Street, Suite 710, Miami, Florida 33128. The County and PAMDC may collectively be referred to herein as "the Parties."

II. PURPOSE

The purpose of this Agreement is to establish the terms and conditions under which MDHCD will provide Housing Choice Voucher (HCV) Landlord Contract Information to the PAMDC for the purpose of facilitating property-related assessments and compliance. The shared information may contain Personally Identifiable Information (PII), which must be protected in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a), and applicable Florida privacy laws.

III. OBLIGATIONS OF THE PARTIES

A. MDHCD OBLIGATIONS

1. MDHCD will provide the PAMDC with HCV Landlord Contract Information, which may include but is not limited to:
    - Landlord names
    - Contract addresses
    - Payment amounts
    - Housing Assistance Payment (HAP) Contracts
    - Participant Name
    - Participant Social Security Number

- Participant Date of Birth
- Lease Agreements

2. MDHCD will provide the data in a secure, encrypted format, via secure file transfer protocols or password-protected files, as mutually agreed upon by the Parties.

B. PAMDC OBLIGATIONS

1. The PAMDC acknowledges that the data provided by MDHCD may contain Personally Identifiable Information (PII) as defined under the Privacy Act of 1974, Florida Statutes, and other applicable data protection laws. Additionally, PAMDC agrees to comply with the legal opinion rendered by the United States Department of Housing and Urban Development's (HUD) Office of General Counsel, dated August 10, 2012, and HUD PIH Notices 2010-15 (HA) and 2015-06, which are attached hereto as Exhibits "A", "B" and "C" and incorporated herein by reference.

2. The PAMDC shall:
   - Use the provided data solely for official property appraisal purposes.
   - Restrict access to the data to employees or agents with a legitimate business need and who are trained in data privacy and security protocols. Accordingly, the PAMDC shall restrict access to the information provided by MDHCD to the following employees or agents:
     (1) Compliance Department Manager;
     (2) Compliance Department Supervisor
     (3) Exemptions and Public Service Director
     (4) Exemptions and Public Service Associate Director
     (5) Senior Counsel, Legal Department
     (6) Chief of Staff and General Counsel
   - Not share, disseminate, or disclose the PII to unauthorized third parties.
3. The PAMDC shall protect all PII by implementing the following security protocols:

IV. SECURITY PROTOCOLS

The PAMDC agrees to the following minimum-security standards to safeguard all PII received under this Agreement:

1. Compliance with Data Encryption:
    - All files containing PII shall be encrypted at rest and in transit using encryption protocols that meet or exceed Federal Information Processing Standards (FIPS) 140-2.
2. Secure Storage:
    - Electronic files shall be stored on secure, access-controlled servers protected by firewalls and regularly updated security software.
    - Physical files (if any) containing PII shall be stored in locked cabinets in areas with restricted access.
3. Access Controls:
    - Access to PII shall be strictly limited to authorized personnel with role-based access controls.
    - All user accounts shall be secured with complex passwords and, where feasible, multi-factor authentication.
4. Breach Notification:
    - The PAMDC shall notify MDHCD immediately, but no later than twenty-four (24) hours after discovery of any actual or suspected security breach involving PII.
    - The PAMDC shall fully cooperate with MDHCD to investigate, mitigate, and resolve the breach, and shall comply with all applicable federal and state breach notification laws, including any requirements to notify affected individuals.
5. Data Retention and Secure Disposal:
    - The PAMDC shall retain PII only as long as necessary to perform its duties under this Agreement.
    - Upon termination of this Agreement or at MDHCD's written request, the PAMDC shall either securely return all PII to MDHCD or destroy it using an approved destruction methods to render it permanently unreadable and unrecoverable.

V. HOLD HARMLESS AND INDEMNIFICATION

The PAMDC agrees to hold harmless, indemnify, and defend MDHCD, its officers, agents, and employees from and against any and all claims, liabilities, losses, damages, costs, and expenses (including attorney's fees) arising out of the PAMDC's unauthorized use or disclosure of PII, any failure to comply with the security obligations set forth in this Agreement, or any breach of this

Agreement by the PAMDC or its personnel. The PAMDC shall pay all claims and losses of any kind in connection therewith and shall investigate and defend all claims, suits or actions of any kind or nature in the name of the County, where applicable, including appellate proceedings, and shall pay all costs, judgments, and attorney's fees which may issue thereon. Notwithstanding the foregoing, this indemnification shall only be to the extent and within the limitations of Section 768.28 Florida Statutes. This provision shall survive the termination of this Agreement.

VI. TERM AND TERMINATION

1. This Agreement shall commence on the date of final signature and shall remain in effect unless terminated by either party with thirty (30) calendar days' prior written notice.
2. Upon termination, the PAMDC shall:
    - Cease all use of the data provided by MDHCD.
    - Return or securely destroy all PII in compliance with the security protocols outlined in this Agreement.

VII. PENALTIES

The Privacy Act provides for criminal penalties for the unauthorized disclosure of Privacy Act protected information to unauthorized third parties. Any person who knowingly or willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be subject to criminal penalties under the Privacy Act and may be subject to prosecution under other statutes such as 18 U.S.C. § 494, § 495, and § 1001. The penalty for violation of the Privacy Act is a fine of not more than $5,000.00. In addition, Parties understand that if they or one of their employees, agents (including contractors or subcontractors), or subrecipients (including an agent or employee of its subrecipients) willfully discloses any such PII to a third party not authorized to receive it or otherwise violates the terms of this Agreement.

VIII. GENERAL PROVISIONS

1. Rights of Third Parties: Except as provided herein, all conditions of the MDHCD, PAMDC and their successors and assigns hereunder are imposed solely and exclusively for the benefit of MDHCD, PAMDC and the United States Department of Housing and Urban Development (HUD), and their successors and assigns, and no other person shall have standing to require satisfaction of such conditions or be entitled to assume MDHCD, PAMDC or HUD will make advances in the absence of strict compliance with any or all conditions of MDHCD, PAMDC or HUD. No other person shall under any circumstances, be deemed to be a beneficiary of this Agreement or any other documents associated with

this Agreement, or any provisions of this Agreement which may be freely waived in whole or in part by MDHCD, PAMDC or HUD at any time if, in their sole discretion, they deem it desirable to do so.

2. Notices: All notices, requests, approvals, demands and other communications given hereunder or in connection with this Agreement shall be in writing and shall be deemed given when delivered by hand or sent by registered or certified mail, return receipt requested, addressed as follows (provided, that any time period for responding to any such communication shall not begin to run until such communication is actually received or delivery is refused):

If to MDHCD:	Miami-Dade County c/o Miami-Dade Housing and Community Development 701 N.W. 1st Court, 16th Floor Miami, Florida 33136 Attn: Nathan Kogan, Director
With a copy to:	Miami-Dade County Attorney's Office 111 N.W. 1st Street, Suite 2810 Miami, Florida 33128 Attn: Terrence A. Smith, Esq. Assistant County Attorney
If to PAMDC:	Property Appraiser of Miami-Dade County 111 N.W. 1st Street, Suite 710 Miami, Florida 33128 Attn: Tomas Regalado, Property Appraiser
With a copy to:	Property Appraiser of Miami-Dade County 111 N.W. 1st Street, Suite 710 Miami, Florida 33128 Attn: Diana Arteaga, Esq. Chief of Staff & General Counsel

3. Governing Law and Venue: This Agreement shall be governed by the laws of the State of Florida and applicable federal privacy laws and applicable regulations. Any dispute arising under, in connection with or related to this Agreement or related to any matter which is the subject of this Agreement shall be subject to the exclusive jurisdiction of the state and/or federal courts in Miami-Dade County, Florida.

4. Entire Agreement: This Agreement represents the entire understanding between the Parties and supersedes all prior agreements or understandings, whether written or oral.

5. Amendments: Any changes to this Agreement must be made in writing and signed by authorized representatives of both Parties.

6. Severability: If any provision of this Agreement is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

[SIGNATURES APPEAR ON THE FOLLOWING PAGES]

VIII. SIGNATURES

IN WITNESS WHEREOF, the Parties have executed this Memorandum of Agreement as of the dates written below.

Miami-Dade County

By: _____
Name: _____
Title: _____
Date: _____

Attest: Juan Fernandez-Barquin
Clerk of the Court and Comptroller

By:_____

(Deputy Clerk's Signature)

Print Name:_____

Date:_____

Approved as to form and legal sufficiency;

By:_____
Assistant County Attorney

Tomas Regalado

Property Appraiser of Miami-Dade County

_____

Date: _____

Approved as to form and legal sufficiency;

By:_____
Diana Arteaga, Esq.
General Counsel, Property Appraiser of Miami-Dade County

U.S. Department of Housing and Urban Development

Atlanta Region, Miami Field Office
Brickell Plaza Federal Building
909 SE First Avenue, Rm. 500
Miami, FL 33131-3042

Exhibit "A"

August 10, 2012

Terrence A. Smith, Esquire
Assistant County Attorney
Office of County Attorney
Miami-Dade County
111 N.W. First Street, Suite 2810
Miami, Florida 33128

Dear Mr. Smith:

This responds to your letter dated July 12, 2012, requesting a legal opinion from the Office of Associate Regional Counsel, Miami Field Office, in the United States Department of Housing and Urban Development ("HUD" or the "Department"). Specifically, your correspondence sought a legal opinion on the applicability of the Federal Privacy Act of 1974 ("Privacy Act' or the "Act") to certain records in the possession of the Miami-Dade County Public Housing and Community Development Department (the "PHCD").

You advised that the PHCD had received several requests for the release of documents for all Section 8 participants pursuant to Florida Statutes, Chapter 119. The documents contain personal information such as participants' addresses, race, ethnicity, disability status, number of children, and cell phone numbers.

Your correspondence also stated that your inquiry was prompted by an apparent conflict between case law and a determination made by the Florida Attorney General on the issue of whether federal or state law applies to the disclosure of certain records maintained by housing authorities. In particular, the court in *Forsberg v. Housing Authority of the City of Miami Beach*, 455 So.2d 373 (Fla. 1984), held that under Florida law, a housing authority's records containing information provided by public housing tenants and prospective tenants were "public records" which were required by the law to be open for public inspection.[1] Similarly, the court in *Housing Authority of City of Daytona Beach v. Gomillion*, 639 So.2d 117 (Fla. 5th DCA 1994), ruled that records maintained on behalf of HUD by a public housing authority were subject to disclosure because the Housing Authority was not an "agency" of the federal government.[2] In contrast, the Florida Attorney General opined that only the responsible federal agency can determine whether federal law preempts Florida public records law, so as to limit control and access to records in the possession of Public Housing Authorities in Florida.[3]

[1] *Forsberg v. Housing Authority of the City of Miami Beach*, 455 So.2d 373 (Fla. 1984).
[2] *Housing Authority of City of Daytona Beach v. Gomillion*, 639 So.2d 117 (Fla. 5th DCA 1994).
[3] Op. Att'y Gen. Fla. (Informal 2006).

Hence, this opinion responds to the question of whether the Federal Privacy Act of 1974 preempts Florida Statute, Chapter 119 thus precluding the PHCD from disclosing documents containing personally identifiable information of Section 8 participants, unless such disclosures fully comply with the requirements of the Federal Privacy Act of 1974.

The Privacy Act does preempt Florida Statute, Chapter 119. As such, the PHCD cannot disclose any documents maintained for Section 8 participants, including documents with personally identifiable information of those participants, unless disclosures comply with the requirements of the Federal Privacy Act of 1974. Moreover, disclosure of these records is also limited by other federal laws such as the Freedom of Information Act ("FOIA").

Unlike the Privacy Act, FOIA and similar federal laws limiting public access to certain records, Florida Public Records Law, known as the Sunshine Law, (Fla. Stat. Chapter 119), authorize greater public access to certain records made or received in connection with the transaction of official business by any public agency created under Florida law. Notwithstanding the access provided by Florida law, "records which would be public under state law are unavailable for public inspection when there is clearly a conflict between federal and state law relating to the confidentiality of records. If the state, (i.e. PHCD, in this case), is subject to a federal statute that requires that certain records remain confidential, then pursuant to the Supremacy Clause of the United States Constitution, Art. VI, U.S. Const., the state must keep the records confidential.[4]

In the instant case, although the PHCD may be subject to Fla. Stat. 119, pursuant to the power granted by Fla. Stat. §421.2[5], the PHCD has entered into several agreements with HUD, including the Annual Contributions Contract, ("ACC"), wherein the PHCD has pledged to comply with "all applicable statutes, executive orders and regulations issued by HUD, and ensure compliance by any contractor or subcontractor engaged for the purposes of performing functions under a contract between the PCHD and HUD.[6] The PHCD is therefore obligated to comply with federal laws, regulations, executive orders etc., with respect to several programs it undertakes on behalf of HUD.

In fact, HUD Notice PIH 2010-15 (HA) advised HUD contractors and third party business partners, such as Public Housing Authorities that they must comply with the provisions of the Privacy Act, as well as FOIA and other federal laws which limit and control dissemination of personally identifiable information. The attached copy of HUD Notice PIH 2010-15 (HA), provides detailed guidance on the PHCD's obligation and responsibilities to protect the privacy of the information that PHAs, "collect, use, maintain and disseminate," on behalf of HUD.

HUD Notice PIH 2010-15 (HA), cites several federal laws which limit and control disclosure of information that PHAs collect on behalf of HUD. These laws include §§42 U.S.C. 1437(d) (q) (4), 42 U.S.C. 1437d, (t) (2) *etc.* of the National Housing Act of 1937 and 24 CFR Part 5. These various statutes and regulations not only require that PHAs comply with the provisions of the Privacy Act,

---

[4] *See* The Government- In-The-Sunshine Manual, (Citations Omitted), (Volume 31, 2009), Part II, available at: http://www.myflsunshine.com/sun/nsf/manual (last visited July 24, 2012).

[5] Fla. Stat. §421.2 authorizes PHAs to *inter alia* "...accept grants or other financial assistance from the Federal Government..., and **to these ends,** to comply with such conditions and enter into such trust indentures, leases or agreements as may be necessary,... [and] **to do any and all things necessary or desirable** to secure the financial aid or cooperation of the Federal Government."

[6] Form HUD-53012A, Section 5.

but also require that all assistance applicants be provided notice informing them of their rights under Privacy Act at the time of application and recertification. HUD's regulation at 24 CFR §5. 212, in particular, addresses compliance with the Privacy Act, namely;

> (a) ***Compliance with the Privacy Act.*** The collection, maintenance, use, and dissemination of SSNs, EINs, any information derived from SSNs and Employer Identification Numbers (EINs), and income information under this subpart shall be conducted, to the extent applicable, in compliance with the Privacy Act (5 U.S.C. 552a) and all other provisions of Federal, State, and local law.
>
> (b) ***Privacy Act notice.*** All assistance applicants shall be provided with a Privacy Act notice at the time of application. All participants shall be provided with a Privacy Act notice at each annual income recertification.

Moreover, the foregoing regulation expressly preempts state law as stated:

> ***Federal preemption.*** This subpart B preempts any State law, including restrictions and penalties, that governs the collection and use of income information to the extent State law is inconsistent with this subpart. 24 CFR Part 5, Subpart B. (*See* 24 CFR §5. 210 (c)).

Furthermore, under the Privacy Act, documents related to Section 8 participants maintained by the PHCD, are "a system of records" maintained by the PHCD on behalf of the Department, to accomplish an agency function. (*See* 5 U.S.C. §552a (a) (3)-(a), 5 U.S.C. §552a (m)). The guidelines governing the Privacy Act of 1974[7] specifies that under 5 U.S.C. §552a (a) (3), "a system of records," also include certain systems operated pursuant to a contract to which the agency is a party."[8] In addition, Subsection §552a (m) of the Act, further clarifies that "systems operated under a contract …designed to accomplish an agency function are, in effect, deemed to be maintained by the agency."[9]Accordingly, documents for Section 8 tenants that the PCHD maintains to accomplish HUD's mandate to develop and provide affordable housing, are essentially, "agency records," whose disclosure is subject to the Privacy Act.

Finally, the Federal Information Security Management Act of 2002, 44 U.S.C. §3541 *et seq*., ("FIMSA"), is another legal basis for the Department's protection, regulation and control of personally identifiable information that is maintained by the PHCD as a consequence of PHCD's role in performing an agency function. Through FISMA, the Department is responsible for;

> "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of; ''(i) information collected or maintained by or on behalf of the agency; and''(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.." (*See*, 44 U.S.C. 3544(a)).

---

[7] 40 Fed. Reg. 28, 948, 951-52, 975-976.
[8] *Id.*
[9] *Id.* at 976.

Therefore, all records in the custody of the PHCD which are collected and maintained by the PHCD on behalf of HUD are subject to security protections and security controls developed and/or adopted by the Department pursuant to the authority of FISMA.

Clearly, as discussed *supra,* federal law expressly preempts state law with respect to the disclosure of the records in question. As such, the PHCD must collect, use, maintain and disseminate the personally identifiable information of Section 8 participants, in a manner that protects the privacy of those applicants, as specified by the foregoing federal laws, including the Privacy Act and FOIA. More importantly, regardless of the Florida Sunshine laws, the system of records maintained by PHCD for Section 8 tenants cannot be disclosed, except that such disclosure is in accordance with the provisions of the Privacy Act, FOIA, FISMA and other applicable federal laws and regulations.

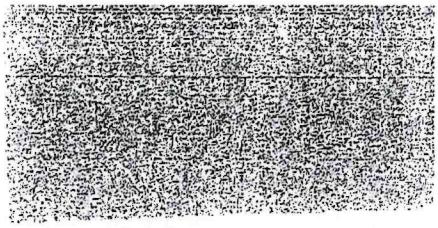
Please contact Sorella Jacobs, Attorney Advisor, at extension 5103 should you need additional guidance or have any questions on this matter.

Sincerely,

Gail Ash Dotson
Associate Regional Counsel

cc: Greg Fortner, Director, PHCD
Annette Molina, Public Information Officer, PHCD
Sharon Matthews Swain, Regional Counsel, Region IV
Jose Cintron, Director, PIH, Miami

Attachment



U.S. Department of Housing and Urban Development
Office of Public and Indian Housing

SPECIAL ATTENTION OF:
Directors of HUD Regional and Field Offices of Public Housing;
Public Housing Agencies that Receive Funds under Any Public and Indian Housing Program

NOTICE PIH 2010- 15 (HA)

Issued: May 6, 2010

Expires: May 31, 2011

Cross References:

Subject: U.S. Department of Housing and Urban Development (HUD) Privacy Protection Guidance for Third Parties

1) **Purpose**: This notice informs all Public Housing Authorities (PHAs) about their responsibilities for safeguarding personally identifiable information (PII) required by HUD and preventing potential breaches of this sensitive data. HUD is committed to protecting the privacy of individuals' information stored electronically or in paper form, in accordance with federal privacy laws, guidance, and best practices. HUD expects its third party business partners, including Public Housing Authorities, who collect, use, maintain, or disseminate HUD information to protect the privacy of that information in accordance with applicable law.

2) **Background**: Section 6 of the Housing Act of 1937, the Privacy Act of 1974, 5 U.S.C. § 552a (Privacy Act), The Freedom of Information Act (FOIA), 5 U.S.C. § 552, and Section 208 of The E-Government Act are the primary federal statutes that limit the disclosure of information about public housing residents and recipients of the Housing Choice Voucher program. In addition, the Housing and Community Development Act of 1987, 42 U.S.C. § 1437d(q)(4), 42 U.S.C. § 1437d (t)(2), 42 U.S.C. § 3543, and the Stewart B. McKinney Homeless Assistance Act of 1988, 42 U.S.C. § 3544, further regulate the treatment of this information.

   a) General HUD program requirements are set forth in 24 C.F.R. Part 5. Compliance with the Privacy Act and other requirements for grants and contracts is spelled out in 24 C.F.R. § 5.212 which states:

      i) *Compliance with the Privacy Act*. The collection, maintenance, use, and dissemination of SSNs, EINs, any information derived from SSNs and Employer Identification Numbers (EINs), and income information under this subpart shall be

conducted, to the extent applicable, in compliance with the Privacy Act (5 U.S.C. 552a) and all other provisions of Federal, State, and local law.

ii) *Privacy Act Notice*. All assistance applicants shall be provided with a Privacy Act notice at the time of application. All participants shall be provided with a Privacy Act notice at each annual income recertification.

The Federal Acquisition Regulation (FAR), 48 C.F. R. Subpart 1524.1, sets forth that compliance with the requirements of the Privacy Act be included in HUD contracts at clause 52.224-2, which provides in part:

...(a) The Contractor agrees to—
(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act ....

Similar language is included in all HUD Grant Agreements requiring the Grantee to comply with the provisions of the Privacy Act of 1974 and the agency rules and regulations issued under the Act. (See Attachments 1 and 2 for the above provisions)

b) Additional federal guidance on privacy protection is in OMB privacy-related memoranda, including:

i) OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
ii) OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
iii) OMB M-04-26, Personal Use Policies and ? File Sharing? Technology
iv) OMB M-05-08, Designation of Senior Agency Officials for Privacy
v) OMB M-06-15, Safeguarding Personally Identifiable Information
vi) OMB M-06-16, Protection of Sensitive Agency Information
vii) OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
viii) OMB Memo, September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification Guidance
ix) OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
x) OMB M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

c) Definitions

As used in this Notice, the following terms are defined as:

i) Personally Identifiable Information (PII). Defined in OMB M-07-16 as ". . . information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

ii) Sensitive Personally Identifiable Information. PII that when lost, compromised or disclosed without authorization could substantially harm an individual. Examples of sensitive PII include social security or driver's license numbers, medical records, and financial account numbers such as credit or debit card numbers.

3) **Guidance on Protecting Sensitive Privacy Information**: The Privacy Act requires that federal agencies maintain only such information about individuals that is relevant and necessary to accomplish its purpose. The Privacy Act also requires that the information be maintained in systems or records – electronic and paper – that have the appropriate administrative, technical, and physical safeguards to protect the information, however current. This responsibility extends to contractors and third party business partners, such as Public Housing Authorities, who are required to maintain such systems of records by HUD.

a) Contractors and third party business partners should take the following steps to help ensure compliance with these requirements:

i) Limit Collection of PII

(1) Do not collect or maintain sensitive PII without proper authorization. Collect only the PII that is needed for the purposes for which it is collected.

ii) Manage Access to Sensitive PII

(1) Only share or discuss sensitive PII with those personnel who have a need to know for purposes of their work. Challenge anyone who asks for access to sensitive PII for which you are responsible.

(2) Do not distribute or release sensitive PII to other employees, contractors, or other third parties unless you are first convinced that the release is authorized, proper and necessary.

(3) When discussing sensitive PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform him/her that the discussion will include sensitive PII.

(4) Never leave messages containing sensitive PII on voicemail.

(5) Avoid discussing sensitive PII if there are unauthorized personnel, contractors, or guests in the adjacent cubicles, rooms, or hallways who may overhear your conversations.

(6) Hold meetings in a secure space (i.e., no unauthorized access or eavesdropping possible) if sensitive PII will be discussed and ensure that the room is secured after the meeting.

(7) Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII.

(8) Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

iii) Protect Hard Copy and Electronic Files Containing Sensitive PII

(1) Clearly label all files containing sensitive PII by placing appropriate physical labels on all documents, removable media such as thumb drives, information systems, and application. Examples of appropriate labels might include ? For Official Use Only? or ? For (Name of Individual/Program Office) Use Only.?

(2) Lock up all hard copy files containing sensitive PII in secured file cabinets and do not leave unattended.

(3) Protect all media (e.g., thumb drives, CDs, etc.,) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.

(4) Keep accurate records of where PII is stored, used, and maintained.

(5) Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.

(6) Secure digital copies of files containing sensitive PII. Protections include encryption, implementing enhanced authentication mechanisms such as two-factor authentication and limiting the number of people allowed access to the files.

(7) Store sensitive PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

iv) Protecting Electronic Transmissions of Sensitive PII via fax, email, etc.

(1) 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, that the fax is in a controlled area, and that all paper waste is disposed of properly (e.g., shredded). When possible, use a fax machine that uses a secure transmission line.

(2) Before faxing PII, coordinate with the recipient so that the PII will not be left unattended on the receiving end.

(3) When faxing sensitive PII, use only individually-controlled fax machines, not central receiving centers.

(4) Do not transmit sensitive PII via an unsecured information system (e.g., electronic mail, Internet, or electronic bulletin board) without first encrypting the information.

(5) When sending sensitive PII via email, make sure both the message and any attachments are encrypted.

(6) Do not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.

v) Protecting Hard Copy Transmissions of Files Containing Sensitive PII

(1) Do not remove records about individuals with sensitive PII from facilities where HUD information is authorized to be stored and used unless approval is first obtained from a supervisor. Sufficient justification, as well as evidence of information security, must been presented.

(2) Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque solid envelopes. Mark the envelope to the person's attention.

(3) When using the U.S. postal service to deliver information with sensitive PII, double-wrap the documents (e.g., use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement ? To Be Opened By Addressee Only.?

vi) Records Management, Retention and Disposition

(1) Follow records management laws, regulations, and policies applicable within your jurisdiction.

(2) Ensure all Public Housing Authority locations and all entities acting on behalf of the Authority are managing records in accordance with applicable laws, regulations, and policies.

(3) Include records management practices as part of any scheduled oversight protocols.

(4) Do not maintain records longer than required.

(5) Destroy records after retention requirements are met.

(6) Dispose of sensitive PII appropriately – use cross-cut shredders or burn bags for hard copy records and permanently erase (not just delete) electronic records.

vii) Incident Response

(1) Supervisors should ensure that all personnel are familiar with reporting procedures.

(2) Promptly report all suspected compromises of sensitive PII related to HUD programs and projects to HUD's National Help Desk at 1-888-297-8689.

4) **Information Contact.** Inquiries about this notice should be directed to Donna Robinson-Staton in the Office of the Chief Information Officer, at 708-5495 ext. 8073.

5) **Paperwork Reduction Act.** The information collection described in this Notice has been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C 3520). In accordance with the PRA, 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.

/s/

Sandra B. Henriquez, Assistant Secretary for
Public and Indian Housing

Attachment 1

The Privacy Act of 1974: http://www.justice.gov/opcl/privstat.htm

Attachment 2

HUD's Implementation of the Privacy Act in 24 CFR Part 16:
http://www.access.gpo.gov/nara/cfr/waisidx_10/24cfr16_10.html

U.S. Department of Housing and Urban Development
Office of Public and Indian Housing

SPECIAL ATTENTION OF:
Directors of HUD Regional and Field Offices of Public Housing;
Public Housing Agencies that Receive Funds under Any Public and Indian Housing Program

NOTICE PIH 2010-15 (HA)

Issued: May 6, 2010

Expires: May 31, 2011

Cross References:

Subject: U.S. Department of Housing and Urban Development (HUD) Privacy Protection Guidance for Third Parties

1) **Purpose**: This notice informs all Public Housing Authorities (PHAs) about their responsibilities for safeguarding personally identifiable information (PII) required by HUD and preventing potential breaches of this sensitive data. HUD is committed to protecting the privacy of individuals' information stored electronically or in paper form, in accordance with federal privacy laws, guidance, and best practices. HUD expects its third party business partners, including Public Housing Authorities, who collect, use, maintain, or disseminate HUD information to protect the privacy of that information in accordance with applicable law.

2) **Background**: Section 6 of the Housing Act of 1937, the Privacy Act of 1974, 5 U.S.C. § 552a (Privacy Act), The Freedom of Information Act (FOIA), 5 U.S.C. § 552, and Section 208 of The E-Government Act are the primary federal statutes that limit the disclosure of information about public housing residents and recipients of the Housing Choice Voucher program. In addition, the Housing and Community Development Act of 1987, 42 U.S.C. § 1437d(q)(4), 42 U.S.C. § 1437d (t)(2), 42 U.S.C. § 3543, and the Stewart B. McKinney Homeless Assistance Act of 1988, 42 U.S.C. § 3544, further regulate the treatment of this information.

   a) General HUD program requirements are set forth in 24 C.F.R. Part 5. Compliance with the Privacy Act and other requirements for grants and contracts is spelled out in 24 C.F.R. § 5.212 which states:

      i) *Compliance with the Privacy Act*. The collection, maintenance, use, and dissemination of SSNs, EINs, any information derived from SSNs and Employer Identification Numbers (EINs), and income information under this subpart shall be

conducted, to the extent applicable, in compliance with the Privacy Act (5 U.S.C. 552a) and all other provisions of Federal, State, and local law.

ii) *Privacy Act Notice*. All assistance applicants shall be provided with a Privacy Act notice at the time of application. All participants shall be provided with a Privacy Act notice at each annual income recertification.

The Federal Acquisition Regulation (FAR), 48 C.F. R. Subpart 1524.1, sets forth that compliance with the requirements of the Privacy Act be included in HUD contracts at clause 52.224-2, which provides in part:

...(a) The Contractor agrees to—
(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act ....

Similar language is included in all HUD Grant Agreements requiring the Grantee to comply with the provisions of the Privacy Act of 1974 and the agency rules and regulations issued under the Act. (See Attachments 1 and 2 for the above provisions)

b) Additional federal guidance on privacy protection is in OMB privacy-related memoranda, including:

i) OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
ii) OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
iii) OMB M-04-26, Personal Use Policies and ? File Sharing? Technology
iv) OMB M-05-08, Designation of Senior Agency Officials for Privacy
v) OMB M-06-15, Safeguarding Personally Identifiable Information
vi) OMB M-06-16, Protection of Sensitive Agency Information
vii) OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
viii) OMB Memo, September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification Guidance
ix) OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
x) OMB M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

c) Definitions

As used in this Notice, the following terms are defined as:

i) Personally Identifiable Information (PII). Defined in OMB M-07-16 as ". . . information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

ii) Sensitive Personally Identifiable Information. PII that when lost, compromised or disclosed without authorization could substantially harm an individual. Examples of sensitive PII include social security or driver's license numbers, medical records, and financial account numbers such as credit or debit card numbers.

3) **Guidance on Protecting Sensitive Privacy Information**: The Privacy Act requires that federal agencies maintain only such information about individuals that is relevant and necessary to accomplish its purpose. The Privacy Act also requires that the information be maintained in systems or records – electronic and paper – that have the appropriate administrative, technical, and physical safeguards to protect the information, however current. This responsibility extends to contractors and third party business partners, such as Public Housing Authorities, who are required to maintain such systems of records by HUD.

a) Contractors and third party business partners should take the following steps to help ensure compliance with these requirements:

i) Limit Collection of PII

(1) Do not collect or maintain sensitive PII without proper authorization. Collect only the PII that is needed for the purposes for which it is collected.

ii) Manage Access to Sensitive PII

(1) Only share or discuss sensitive PII with those personnel who have a need to know for purposes of their work. Challenge anyone who asks for access to sensitive PII for which you are responsible.

(2) Do not distribute or release sensitive PII to other employees, contractors, or other third parties unless you are first convinced that the release is authorized, proper and necessary.

(3) When discussing sensitive PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform him/her that the discussion will include sensitive PII.

(4) Never leave messages containing sensitive PII on voicemail.

(5) Avoid discussing sensitive PII if there are unauthorized personnel, contractors, or guests in the adjacent cubicles, rooms, or hallways who may overhear your conversations.

(6) Hold meetings in a secure space (i.e., no unauthorized access or eavesdropping possible) if sensitive PII will be discussed and ensure that the room is secured after the meeting.

(7) Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII.

(8) Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

iii) Protect Hard Copy and Electronic Files Containing Sensitive PII

(1) Clearly label all files containing sensitive PII by placing appropriate physical labels on all documents, removable media such as thumb drives, information systems, and application. Examples of appropriate labels might include ? For Official Use Only? or ? For (Name of Individual/Program Office) Use Only.?

(2) Lock up all hard copy files containing sensitive PII in secured file cabinets and do not leave unattended.

(3) Protect all media (e.g., thumb drives, CDs, etc.,) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.

(4) Keep accurate records of where PII is stored, used, and maintained.

(5) Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.

(6) Secure digital copies of files containing sensitive PII. Protections include encryption, implementing enhanced authentication mechanisms such as two-factor authentication and limiting the number of people allowed access to the files.

(7) Store sensitive PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

iv) Protecting Electronic Transmissions of Sensitive PII via fax, email, etc.

(1) 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, that the fax is in a controlled area, and that all paper waste is disposed of properly (e.g., shredded). When possible, use a fax machine that uses a secure transmission line.

(2) Before faxing PII, coordinate with the recipient so that the PII will not be left unattended on the receiving end.

(3) When faxing sensitive PII, use only individually-controlled fax machines, not central receiving centers.

(4) Do not transmit sensitive PII via an unsecured information system (e.g., electronic mail, Internet, or electronic bulletin board) without first encrypting the information.

(5) When sending sensitive PII via email, make sure both the message and any attachments are encrypted.

(6) Do not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.

v) Protecting Hard Copy Transmissions of Files Containing Sensitive PII

(1) Do not remove records about individuals with sensitive PII from facilities where HUD information is authorized to be stored and used unless approval is first obtained from a supervisor. Sufficient justification, as well as evidence of information security, must been presented.

(2) Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque solid envelopes. Mark the envelope to the person's attention.

(3) When using the U.S. postal service to deliver information with sensitive PII, double-wrap the documents (e.g., use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement ? To Be Opened By Addressee Only.?

vi) Records Management, Retention and Disposition

(1) Follow records management laws, regulations, and policies applicable within your jurisdiction.

(2) Ensure all Public Housing Authority locations and all entities acting on behalf of the Authority are managing records in accordance with applicable laws, regulations, and policies.

(3) Include records management practices as part of any scheduled oversight protocols.

(4) Do not maintain records longer than required.

(5) Destroy records after retention requirements are met.

(6) Dispose of sensitive PII appropriately – use cross-cut shredders or burn bags for hard copy records and permanently erase (not just delete) electronic records.

vii) Incident Response

(1) Supervisors should ensure that all personnel are familiar with reporting procedures.

(2) Promptly report all suspected compromises of sensitive PII related to HUD programs and projects to HUD's National Help Desk at 1-888-297-8689.

4) **Information Contact.** Inquiries about this notice should be directed to Donna Robinson-Staton in the Office of the Chief Information Officer, at 708-5495 ext. 8073.

5) **Paperwork Reduction Act.** The information collection described in this Notice has been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C 3520). In accordance with the PRA, 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.

/s/

Sandra B. Henriquez, Assistant Secretary for
Public and Indian Housing

Attachment 1

The Privacy Act of 1974: http://www.justice.gov/opcl/privstat.htm

Attachment 2

HUD's Implementation of the Privacy Act in 24 CFR Part 16:
http://www.access.gpo.gov/nara/cfr/waisidx_10/24cfr16_10.html

U.S. Department of Housing and Urban Development
Office of Public and Indian Housing

SPECIAL ATTENTION OF:
Directors of HUD Regional and Field Offices of Public Housing;
Public Housing Agencies that Receive Funds under Any Public and Indian Housing Program

NOTICE PIH-2015-06

Issued: April 23, 2015

Expires: Effective until amended, superseded, or rescinded

Cross References:
PIH 2014-10, PIH 2010-15

Subject: U.S. Department of Housing and Urban Development (HUD) Privacy Protection Guidance for Third Parties

1) **Purpose**: This notice informs all public housing agencies (PHAs) about their responsibilities for safeguarding personally identifiable information (PII) required by HUD and preventing potential breaches of this sensitive data. HUD is committed to protecting the privacy of individuals' information stored electronically or in paper form, in accordance with federal privacy laws, guidance, and best practices. HUD expects its third party business partners, including Public Housing Authorities, who collect, use, maintain, or disseminate HUD information to protect the privacy of that information in accordance with applicable law.

   PIH 2014-14 is being revised to include guidance to assist PHA system administrators and users to fulfill their requirements for information technology security awareness training.

2) **Background**: Section 6 of the Housing Act of 1937, the Privacy Act of 1974, 5 U.S.C. § 552a (Privacy Act), The Freedom of Information Act (FOIA), 5 U.S.C. § 552, and Section 208 of The E-Government Act are the primary federal statutes that limit the disclosure of information about public housing residents and recipients of the Housing Choice Voucher program. In addition, the Housing and Community Development Act of 1987, 42 U.S.C. § 1437d (q)(4), 42 U.S.C. § 1437d (t)(2), 42 U.S.C. § 3543, and the Stewart B. McKinney Homeless Assistance Act of 1988, 42 U.S.C. § 3544, further regulate the treatment of this information.

   a) General HUD program requirements are set forth in 24 C.F.R. Part 5, Subpart B, Disclosure and Verification of Social Security Numbers and Employer Identification Numbers: Procedures for Obtaining Income Information. Subpart B enables HUD and

PHAs to obtain income information about applicants and participants in the covered programs through computer matches with State Wage Information Collection Agencies (SWICAs) and Federal agencies, in order to verify an applicant's or participant's eligibility for or level of assistance.

i) *Restrictions on Use of Income Information Obtained from SWICA and Federal Agencies.* The restrictions of 42 U.S.C. 3544(c)(2)(A) apply to the use by HUD or a PHA of income information obtained from a SWICA and the restrictions of 42 U.S.C. 3544(c)(2)(A) and of 26 U.S.C. 6103(l)(7)(C) apply to the use by HUD or a PHA of income information obtained from the Internal Revenue Service or the Social Security Administration.

b) The Privacy Act and other requirements for grants and contracts is spelled out in 24 C.F.R. 5.212 which states:

i) *Compliance with the Privacy Act.* The collection, maintenance, use, and dissemination of SSNs, EINs, any information derived from SSNs and Employer Identification Numbers (EINs), and income information under this subpart shall be conducted, to the extent applicable, in compliance with the Privacy Act (5 U.S.C. 552a) and all other provisions of Federal, State, and local law.

Privacy Act Notice. All assistance applicants shall be provided with a Privacy Act notice at the time of application. All participants shall be provided with a Privacy Act notice at each annual income recertification.

c) The Federal Acquisition Regulation (FAR), 48 C.F.R. 24.104, sets forth that compliance with the requirements of the Privacy Act be included in HUD contracts at clause 52.224-2, which provides in part:

(a) The Contractor agrees to—
(1) *Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act ....*

Similar language is included in all HUD Grant Agreements requiring the Grantee to comply with the provisions of the Privacy Act of 1974 and the agency rules and regulations issued under the Act. (See Attachments 1 and 2 for the above provisions)

d) Additional federal guidance on privacy protection is in OMB privacy-related memoranda, including:

i) OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy

ii) OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

iii) OMB M-04-26, Personal Use Policies and —File Sharing Technology

iv) OMB M-05-08, Designation of Senior Agency Officials for Privacy

v) OMB M-06-15, Safeguarding Personally Identifiable Information

vi) OMB M-06-16, Protection of Sensitive Agency Information

vii) OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

viii) OMB Memo, September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification Guidance

ix) OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

x) OMB M-14-04, FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (FISMA). FISMA requires federal agencies to implement a mandatory set of processes designed to ensure the confidentiality, integrity, and availability of system related information. FISMA requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely, and efficient manner.

e) Definitions

As used in this Notice, the following terms are defined as:

i) Personally Identifiable Information (PII). Defined in OMB M-07-16 as ". . . information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

ii) Sensitive Personally Identifiable Information. PII that when lost, compromised or disclosed without authorization could substantially harm an individual. Examples of sensitive PII include social security or driver's license numbers, medical records, and financial account numbers such as credit or debit card numbers.

3) **Guidance on Protecting Sensitive Privacy Information**: The Privacy Act requires that federal agencies maintain only such information about individuals that is relevant and necessary to accomplish its purpose. The Privacy Act also requires that the information be maintained in systems or records – electronic and paper – that have the appropriate

administrative, technical, and physical safeguards to protect the information, however current. This responsibility extends to contractors and third party business partners, such as Public Housing Authorities, who are required to maintain such systems of records by HUD.

a) Contractors and third party business partners should take the following steps to help ensure compliance with federal requirements:

i) Security Awareness and Privacy Training

(1) The National Institute of Standards and Technology (NIST) publishes templates and guides for what security awareness trainings should entail in order to be FISMA compliant. These guidelines focus on the following key aspects:

- **Confidentiality** - Protecting information from unauthorized access and disclosure.
- **Integrity** - Assuring the reliability and accuracy of information and IT resources by guarding against unauthorized information modification or destruction.
- **Availability** - Defending information systems and resources to ensure timely and reliable access and use of information. As such, systems are vulnerable to misuse, interruptions and manipulation.
- **Threat**- A threat in the case of IT security is the potential to cause unauthorized disclosure, unavailability, changes, or destruction of protected information.
- **Vulnerability**- Any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy
- **Risk** is the likelihood that a threat will exploit vulnerability.
- **Controls** are policies, procedures, and practices designed to decrease the likelihood, manage the impact, or minimize the effect of a threat exploiting a vulnerability

(2) Additionally, the NIST provides publications for reference on Building an Information Technology Security Awareness and Training Program and Security and Privacy Controls for Federal Information Systems and Organizations

(3) PHAs should maintain adequate documentation that supports the training for all staff as well as maintain auditable records of training completion. Although there is not required reporting on the training, Office of Field Operations personnel may spot-check compliance on on-site visits.

ii) Limit Collection of PII

(1) Do not collect or maintain sensitive PII without proper authorization. Collect only the PII that is needed for the purposes for which it is collected.

(2) Consistent with the provisions of this Notice, PHAs may enter into agreements (or in some cases be required) to provide PII to legitimate researchers under contract

or other agreement with HUD to support studies on the effects and operations of HUD programs. Further, HUD encourages PHAs to supply PII to other legitimate researchers who do not have contracts or other agreements with HUD in support of such studies, so long as the PHA in question has taken reasonable precautions to prevent disclosure of PII outside of the research team. Such reasonable precautions generally involve written agreements between the PHA and one or more researchers that specify the legal obligations of the latter to protect PII from disclosure.

iii) Manage Access to Sensitive PII

(1) Only share or discuss sensitive PII with those personnel who have a need to know for purposes of their work. Challenge anyone who asks for access to sensitive PII for which you are responsible.

(2) Do not distribute or release sensitive PII to other employees, contractors, or other third parties unless you are first convinced that the release is authorized, proper and necessary.

(3) When discussing sensitive PII on the telephone, confirm that you are speaking to the right person before discussing the information and inform him/her that the discussion will include sensitive PII.

(4) Never leave messages containing sensitive PII on voicemail.

(5) Avoid discussing sensitive PII if there are unauthorized personnel, contractors, or guests in the adjacent cubicles, rooms, or hallways who may overhear your conversations.

(6) Hold meetings in a secure space (i.e., no unauthorized access or eavesdropping possible) if sensitive PII will be discussed and ensure that the room is secured after the meeting.

(7) Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII.

(8) Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

iv) Protect Hard Copy and Electronic Files Containing Sensitive PII

(1) Clearly label all files containing sensitive PII by placing appropriate physical labels on all documents, removable media such as thumb drives, information systems, and application. Examples of appropriate labels might include —For Official Use Only or —For (Name of Individual/Program Office) Use Only.

(2) Lock up all hard copy files containing sensitive PII in secured file cabinets and do not leave unattended.

(3) Protect all media (e.g., thumb drives, CDs, etc.,) that contain sensitive PII and do not leave unattended. This information should be maintained either in secured file cabinets or in computers that have been secured.

(4) Keep accurate records of where PII is stored, used, and maintained.

(5) Periodically audit all sensitive PII holdings to make sure that all such information can be readily located.

(6) Secure digital copies of files containing sensitive PII. Protections include encryption, implementing enhanced authentication mechanisms such as two-factor authentication, and limiting the number of people allowed access to the files.

(7) Store sensitive PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

v) Protecting Electronic Transmissions of Sensitive PII via fax, email, etc.

(1) 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, that the fax is in a controlled area, and that all paper waste is disposed of properly (e.g., shredded). When possible, use a fax machine that uses a secure transmission line.

(2) Before faxing PII, coordinate with the recipient so that the PII will not be left unattended on the receiving end.

(3) When faxing sensitive PII, use only individually-controlled fax machines, not central receiving centers.

(4) Do not transmit sensitive PII via an unsecured information system (e.g., electronic mail, Internet, or electronic bulletin board) without first encrypting the information.

(5) When sending sensitive PII via email, make sure both the message and any attachments are encrypted.

(6) Do not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.

vi) Protecting Hard Copy Transmissions of Files Containing Sensitive PII

(1) Do not remove records about individuals with sensitive PII from facilities where HUD information is authorized to be stored and used unless approval is first obtained from a supervisor. Sufficient justification, as well as evidence of information security, must been presented.

(2) Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque solid envelopes. Mark the envelope to the person's attention.

(3) When using the U.S. postal service to deliver information with sensitive PII, double-wrap the documents (e.g., use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement —To Be Opened By Addressee Only.

vii) Records Management, Retention, and Disposition

(1) Follow records management laws, regulations, and policies applicable within your jurisdiction.

(2) Ensure all Public Housing Authority locations and all entities acting on behalf of the Authority are managing records in accordance with applicable laws, regulations, and policies.

(3) Include records management practices as part of any scheduled oversight protocols.

(4) Do not maintain records longer than required.

(5) Destroy records after retention requirements are met.

(6) Dispose of sensitive PII appropriately – use cross-cut shredders or burn bags for hard copy records and permanently erase (not just delete) electronic records.

viii) Incident Response

(1) Supervisors should ensure that all personnel are familiar with reporting procedures.

(2) Promptly report all suspected compromises of sensitive PII related to HUD programs and projects to HUD's National Help Desk at 1-888-297-8689.

ix) Contact Information

Inquiries about this notice should be directed to Matthew Steen, Privacy Liaison Officer, Real Estate Assessment Center, Office of Public and Indian Housing, at 202-475-8933.

x) **Paperwork Reduction Act**. The information collection described in this Notice has been approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C 3520). In accordance with the PRA, 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.

/s/

Lourdes Castro Ramírez,
Principal Deputy Assistant Secretary for
Public and Indian Housing