
Reminder of Enterprise Income Verification (EIV) System Data Disclosure and Safeguards

Owners, Management Agents, and Contract Administrators for HUD Multifamily Housing properties are reminded of the following information relating to the security of EIV System Data.

Authorized Disclosure

Only entities or individuals authorized by the Social Security Act and identified in HUD's Computer Matching Agreement are permitted to view EIV data, regardless of format (e.g. hard copy, soft copy, systems). Authorized entities are:

- Owners, in connection with the administration of Multifamily Housing programs;
- Contract Administrators (PBCAs and TCAs) and HUD staff;
- Independent Public Auditors **;
- OIG investigators for auditing purposes; and
- Individuals assisting in the recertification process and who are present during the recertification interview and process.

** Independent public auditor (IPA) is a Certified Public Accountant or a Public Auditor licensed or registered public accountant, having no business relationship with the private owner except for the performance of audit, systems work and tax preparation. If not certified, the Public Accountant must have been licensed or registered by a regulatory authority of a State or other political subdivision of the United States on or before December 31, 1970. In States that do not regulate the use of the title "public accountant," only Certified Public Accountants may be used.

Note: The definition of IPA does not include other consultants hired by an O/A to audit tenant files for compliance.

Rules of Behavior and The Federal Privacy Act

The Federal Privacy Act (5 USC 552a, as amended) prohibits the disclosure of an individual's personal information to another person without the written consent of such individual. This consent is gained through completion of form HUD-9887/9887a. The data in the EIV system contains personal information on individual tenants that is covered by the Privacy Act. EIV data must only be disclosed for official purposes in accordance with the Rules of Behavior (ROB).

The ROB must be signed by owner and management agent staff, HUD staff, and CA staff who do not have access to the EIV system but who view or use EIV data/reports provided by authorized EIV Coordinators or EIV Users in order to perform their job functions. The ROB must be made available upon request to the entity monitoring EIV system compliance.

Safeguards

The data provided via the EIV system must be safeguarded to ensure that it is only used for official purposes and not disclosed in any way that would violate the privacy of the individuals represented in the system data. Practices and controls must be developed by HUD and program administrators to secure information are grouped into three types of safeguards:

- Technical safeguards: User identification and authentication, ensuring only those who have a need to use the EIV system to perform their job function have access to the EIV system, and security training;
- Administrative safeguards: Established policies and procedures that govern the use of the EIV system; and
- Physical safeguards: Physical measures taken to ensure data is safe when stored electronically or in hardcopy.

Sanctions

- Willful unauthorized disclosure or inspection of EIV Data can result in the following:
- Unauthorized Disclosure – felony conviction and fine up to \$5,000 or imprisonment up to five (5) years, as well as civil damages.
- Unauthorized Inspection – misdemeanor penalty of up to \$1,000 and/or one (1) year imprisonment, as well as civil damages

Disclosures and safeguards of EIV data is further discussed in HUD Handbook 4350.3 REV-1, Chapter 9.
