

# Sample EIV Privacy Policy

Property \_\_\_\_\_

Print Name \_\_\_\_\_

## Employee/Agent Type

Certification/Management Staff  Compliance Staff  Contract Administrator  Other \_\_\_\_\_

You are required to review and acknowledge the information in this document because you are being provided with access to an area that contains confidential resident information. Unauthorized access or disclosure of information is a federal offense punishable by substantial fines and/or incarceration.

It is the policy of the owner/agent to guard the privacy of applicants and residents conferred by the Federal Privacy Act of 1974 and the Health Insurance Portability & Accountability Act of 1996 (HIPAA) to ensure the protection of such individuals' records maintained by the owner/agent. Therefore the owner/agent shall not disclose any personal information contained in its records to any outside person or agency unless the individual about whom information is requested shall give written consent to such disclosure.

*(Note: This does not include persons responsible for eligibility determination or compliance monitoring such as HUD or HUD's agents. Information is provided to HUD and HUD's agents on a regular basis in order to assure compliance and timely payment of housing assistance payments. In addition, in cases of suspected fraud, information may be provided to the Office of the Inspector General or others as directed by subpoena or court order.)*

This Privacy Policy in no way limits the owner/agent's ability to collect such information, as it may need, to determine eligibility, compute rent, or determine an applicant's eligibility or suitability for tenancy. Consistent with the intent of Section 504 of the Rehabilitation Act of 1973, any information obtained regarding a person's disability will be treated in a confidential manner. We are dedicated to protecting the privacy of personal information that was used to determine eligibility for rental assistance based on HUD regulations, including Social Security, other governmental identification numbers and any other required information. We have adopted a privacy policy to help ensure that information is kept secure.

**Technical safeguards: Only HUD or HUD's agents and authorized staff have access rights to information based on their role in the company. These roles are monitored on a regular basis through inspections and reviews. Authorization procedures for staff will:**

1. Reduce the risk of a security violation related to the EIV system's software, network, or applications
2. Identify and authenticate all users seeking to use the EIV system data
3. Deter and detect attempts to access the system without authorization
4. Monitor the user activity on the EIV system

**Administrative Safeguards:** Staff is trained based on federal and state laws regarding privacy. Written policies and procedures include but are not limited to making sure that the HUD required 9887, 9887A and consents are updated and in place. File audits completed internally as well as HUD reviews help to ensure compliance with these policies. These administrative procedures will:

1. Ensure that access rights, roles, and responsibilities are appropriately and adequately assigned
2. Protect copies of sensitive data and destroy system-related records to prevent reconstruction of the contents
3. Ensure authorized release of resident information consent form is included in all family files, before accessing and using data
4. Maintain, communicate, and enforce policies related to securing EIV data
5. Train staff on security measures and awareness, preventing the unauthorized accessibility and use of data

# Sample EIV Privacy Policy

Property \_\_\_\_\_

**Physical Safeguards:** The owner/agent will document all persons who have access to resident data or who have permission to enter areas where resident data is stored. Such persons are required to review and acknowledge the Privacy Act Requirements and must agree to comply with these requirements.

Staff is required to notify Coordinators/Security Administrators of system breaches and penetration by unauthorized users. There are written policies which include all personal information to be kept in a locked file cabinet, certain printer/fax/electronic equipment designated to receive confidential information and system security to prevent security breaches. These physical safeguards will:

1. Establish barriers between unauthorized persons and documents/computer media containing private data.
2. Clearly identify restricted areas by use of prominently posted signs or other indicators.
3. Develop a list of authorized users who can access restricted areas-e.g., contractors, maintenance, and janitorial/cleaning staff.
4. Prevent undetected entry into protected areas and/or documents with posted signage that reads "authorized personnel only".
5. Ensure that any electronic versions of resident data are stored in a separate password protected director
6. Ensure that all electronic versions of resident data are encrypted
7. Ensure all emails that include confidential resident data are encrypted

**Disposal of Information:** In accordance with the FTC "Disposal of Consumer Report Information and Record", any applicant/resident files that are destroyed based on the Records Retention Policy will be disposed properly. Proper disposal of this information is one that is reasonable and appropriate to prevent unauthorized access to personal information such as the items listed above. Approved disposal methods are:

- Burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;
- Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed;
- Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule.

Keeping applicant and resident information confidential is one of our most important responsibilities. We maintain physical, electronic and procedural safeguards to protect information. We are bound by a code of ethics that requires confidential treatment of eligibility information and are subject to disciplinary action if this code is not followed.

Please feel free to contact the management team at any time to discuss our Privacy Policy or anything else that will help ensure our residents continued enjoyment in their home with us.

**Property Name** \_\_\_\_\_

I have read and understand the Privacy Act requirements and agree to comply, under penalty of law.  Yes  No

I have received keys allowing me to access areas where confidential information is maintained.  Yes  No

If yes. Date key provided: \_\_\_\_\_ Initials: \_\_\_\_\_

Number of keys: \_\_\_\_\_ Initials: \_\_\_\_\_

**Signed:** \_\_\_\_\_

Date key(s) returned: \_\_\_\_\_ Initials: \_\_\_\_\_

Acknowledgement of key return: Initialed by property manager \_\_\_\_\_

