Resident Privacy: Protocols and Policy

This document outlines the privacy expectations and commitment regarding the protection of resident data and information. These protocols and policy apply to all staff that collect, analyze or otherwise interface with resident data and personal information.

Overview

National Housing Trust (NHT) is committed to protecting the privacy and rights of residents living in NHT communities. As such, specific guidelines around this protection is outlined in this document to ensure a standard policy is followed. This document will outline:

- The purpose of resident data collection,
- Practices around the protection, collection and proper elimination of sensitive data(including those not required under federal law),
- System ownership, maintenance and security, as well as
- Resident consent and participation regarding data collection.

For the purposes of this document, an authorized agent is defined as an individual or group of individuals who has agreed in writing to NHT's Resident Privacy Protocols and who acts on behalf of the National Housing Trust. This includes property management companies, vendors, and relevant community stakeholder.

Purpose of Resident Data Collection

Goal: Clearly state the purpose for resident data collection as it relates to the provision of services and/or programming.

NHT is committed to protecting the privacy of residents' personal information and will acquire, collect, use and/or disclose this information only as permitted by applicable federal and state law. As needed to perform their job duties and as permitted by applicable law, NHT staff and authorized agents may, without resident authorization, use and share personal information between each party. This includes annual resident demographic collection for each community by NHT staff. NHT staff and authorized agents who have no business need to access or use resident personal information may not access this information. This information will be used only for the purposes of which it was created or collected.

When accessing resident personal information, NHT staff and authorized agents will utilize only the data that is necessary to complete the related task and maintain its privacy both during and after its use. This means personal information should not be discussed in public areas, personal information in written form should not be left public place where others can easily access it, and appropriate steps will be made to identify data as confidential to ensure privacy.

Best Practices for Data Collection, Retention and Elimination

Goal: Specify how to appropriately collect and protect resident data, including how to properly store, secure and rid of data according to federal and state regulations, as well as FIPPs.

When collecting resident data, NHT staff and authorized agents will use both federal and state regulation and, where no legal definition applies, the Fair Information Practice Principles (FIPPs) to guide data privacy standards.

1101 30th Street, NW Suite 100a
Washington, DC 200007

202-333-8931 (Phone)
202-833-1031 (Fax)

www.nationalhousingtrust.org

FIPPs are a set of internationally recognized practices for addressing the privacy of information about individuals, and provide the underlying policy for many national laws addressing privacy and data protection matters. Under FIPPs, data will be utilized with transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security and accountability and auditing. Under federal and state laws, there are several data points that necessitate protection and privacy regarding its usage. These data points include, but are not limited to:

General information

In general, aggregate resident data is collected across a community to inform an understanding of the resident population. Because this information is collected in aggregate and not connected to an individual or group of individuals, it is typically not considered 'sensitive' information; however, NHT staff and authorized agents will protect this personal information under the FIPPs guidelines.

Financial Information

This information could include:

- Financial account information (bank account, or lack thereof)
- Rent payment history
- Income and employment information
- Certain laws that may apply to this information includes:
- Fair Credit Reporting Act (FCRA): promotes accuracy, fairness and the privacy of personal information assembled by Credit Reporting Agencies (CRAs).

Health Information

This information could include:

- Information about mental pr physical health status or treatment (such as ER visits, primary care provider, depression screenings, etc.)
- Substance abuse history or treatment information
- Insurance information

Certain laws that may apply to this information includes:

- Data this is **individually identifiable**. (de-identified or aggregate data does not count, but must be truly de-identified).
- HIPPA-regulated data, **if** collected by a health care provider, health insurance plan or by a service provider working on behalf of a provider or plan.
- If information is collected directly from tenants, there is looser restrictions around how this data is regulated; however, transparency around data collection and usage will be communicated with residents.

Education Information

This information could include:

- Education level of adults
- Enrollment in HeadStart or grade advancement for children

Certain laws that may apply to this information includes:

- The Family Education Rights and Privacy Act (FERPA): protects the privacy of educational records maintained by schools that receive federal funds.

Information about Children

This information could include:

- Can also be health or education information

Certain laws that may apply to this information includes:

- The Children's Online Privacy Protection Act (COPPA): protects the privacy of information about children on the internet.

Housing Stability information

This type of personal information is not generally covered by federal regulations; however, will comply with FIPPs guidelines. This information could include:

- Turnover rate
- Households that move and why (such as an eviction, home purchase, property transfer, etc.)

Community Engagement

This type of personal information is not generally covered by federal regulations; however, will comply with FIPPs guidelines. This information could include:

- Feelings about safety
- Voter registration

Resident Consent and Participation

Goal: Outline the protocols to obtain resident consent and participation in the sharing of personal data and information for the purposes of community programming and services through both internal and external uses.

To ensure clear communication of its usage, NHT staff and authorized agents will provide information to residents about the use and disclosure of their personal information. Where required by law, NHT staff and authorized agents will inform the resident whenever personal information is requested, whether the disclosure is mandatory, the main purpose for the use of the personal information and the routine uses of the personal information. NHT staff and authorized agents will disclose resident personal information to third parties only in accordance with a resident's written authorization or as permitted or required by applicable law. Examples of situations in which personal information may be disclosed without a resident's authorization include, but are not limited to:

- Vulnerable adult and maltreatment of minors reporting
- Other disclosures to government agencies in accordance with applicable law
- Disclosures to prevent harm to other residents or individuals
- Disclosure to vendors and NHT who need personal information to provide services to NHT.

System Ownership, Maintenance and Security

Goal: Clearly identify who within and outside of the org may access resident data, what circumstances may permit this type of access and how information is appropriately shared.

NHT staff and authorized agents will provide security for resident personal information in accordance with applicable law. This includes taking the steps to (1) maintain the confidentiality, integrity and availability of the information, (2) protect

against any reasonably anticipated threats or hazards to the security or integrity of such information (including ease of access), and (3) protect against any reasonably anticipated use of disclosures of such information that are not permitted or required. Each community manager will be responsible for overseeing the proper use of resident personal information, including its security.

To date, each property management company and NHT's Community Outreach and Impact (COI) team are the sole collectors of resident personal information. This information is collected upon resident move-in, renewal and recertification periods as necessary and relevant to applicable law, in addition to participation in COI-led programs and services. All data is stored in an electronic database that is managed by the information and technology (IT) team of the property management company. Transfer of information is shared both electronically and by paper. NHT staff and authorized agents should minimize the use of paper files, especially during travel.

Under no circumstances should resident personal information be saved to a personal device, either by an agent of the property management company, NHT staff or a separate authorized agent. If NHT learns of an unauthorized use, access or disclosure of resident personal information, NHT will investigate the incident to determine whether it violates applicable law and if any notification to the individual or government agency is advisable or legally required. During this investigation, NHT will review the following:

- The nature and extent of the information involved, including the types of identifiers and likelihood of re-identification,
- The unauthorized person who used the information or to whom the disclosure was made,
- Whether the information was actually acquired or viewed, and
- The extent to which the risk to the information or the resident has been mitigated.

If notification is advisable or legally required, NHT's Asset Manager will coordinate with the community manager to oversee the preparation and submission of the notice, and report on the final outcome to NHT's senior leadership.

NHT staff and authorized agents, including property management staff, with access to the records of resident personal information will ensure that all information is securely destroyed. For paper records, this includes methods such as shredding to ensure the information is rendered unreadable and unable to be reconstructed. Paper redaction is not considered a secure method of disposal. For electronic information, NHT staff and authorized agents, including property management staff, will complete the following:

- Overwrite files with non-sensitive data,
- Purge files that are no longer in use, including permanent deletion (deleting the file and then deleting the contents of a Recycle Bin),
- Electronic redaction with password-protection, or
- Electronic shredding through third-party programming.