Protecting & Storing Client Data

Policy: Data Management and Security

Next: HMIS User Access And Security Settings

This policy establishes and documents standard operating procedures for ensuring the privacy and security of client data used by Anything Helps, thereby protecting sensitive information of individuals experiencing homelessness and ensuring compliance with privacy laws and organizational protocols.

Definitions

Homeless Management Information System (HMIS) - A system used to collect data on the provision of housing and services to homeless individuals and families.

Clarity Human Services: The cloud-based software system selected to manage and report county data for organizations that provide homeless services.

Personally Identifiable Information (PII) - Data that can be used to distinguish an individual’s identity. This includes general and sensitive PII.

- General PII - Includes a client's name, date of birth, social security number, address, and biometric information, such as photographs.
- Sensitive PII - Information that, in combination with identity elements, could pose a risk to clients if disclosed or misused. This information is collected for all clients but is protected and used strictly for legitimate business purposes.

Encrypted Devices: Devices that use encryption to prevent unauthorized access to data stored on the device.

Procedures

Collecting Data

- Conduct skilled and sensitive interviews to collect data and enter it directly during the interview whenever possible.
- If data is collected on paper, enter it into the system the same day to maintain accuracy and avoid data entry errors.

Securing Data

- Store client data only on encrypted devices or in locked file cabinets.
- When traveling, always take laptops or mobile devices with you and do not leave them in unsecure locations.
- When traveling, always take laptops or mobile devices with you and do not leave them in unsecured locations.
- Avoid downloading or transferring data unless necessary. Delete client identifiers if not needed.
- Design memorable passwords, store them securely if written down, and ensure devices are locked when not in use.
- Do not leave screens with PII open on computers when stepping away or if others can see your screen.

Sharing Data

- Never send identifying data via unencrypted email, text, or any other unencrypted electronic methods. Only use HMIS unique identifiers when referring to clients via unencrypted channels.
- Share PII only with authorized personnel who have a legitimate need to know.
- When responding to outside inquiries, do not provide, confirm, or deny any information that could be used to determine the identity, history, or location of the client.

Handling and Disposing of Data

- Electronically shred or otherwise destroy files with client data when no longer needed or when a computer is no longer in use.
- Report inadvertent sharing or breaches of protected data immediately to the King County System Administrator and involve your supervisor, HMIS security officer, and appropriate management personnel.

Compliance and Monitoring

- The Lead Administrator will conduct semi-annual reviews using the Security Compliance Checklist to ensure compliance with these procedures and will take corrective actions as necessary.