MEALS on WHEELS
NORTH CENTRAL TEXAS

PRIVACY & SECURITY POLICY

Our **Privacy & Security Policy** refers to our commitment to treat information of employees, clients, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently, and with respect towards individual rights.

Meals on Wheels North Central Texas Inc (MOWNCT) will work in cooperation with Texas Health and Human Services (Texas HHS) agencies' or federal regulatory inspections, audits, or investigations related to compliance with the Data Use Agreement (DUA) or applicable law.

MOWNCT will secure partners to assist with oversight in regards to information technology and data management.

Authorized users will comprise of Controller, Client Services Director, Case Managers, Accounting-IS Specialist, and Receptionist for the purpose to authorize to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze confidential information.

As part of our operations, MOWNCT will need to obtain and process minimal information. This minimal information may include any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data, etc. MOWNCT collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available the following guidelines apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Protected against any unauthorized or illegal access by internal or external parties
- Only permit Authorized Users with up-to-date privacy and security training, and with a reasonable and demonstrable need to use, disclose, create, receive, maintain, access or transmit the Texas HHS Confidential Information, to carry out an obligation under the DUA for an Authorized Purpose, unless otherwise approved in writing by a Texas HHS agency.

Our data will not be:

- Transferred to organizations, states, or countries that do not have adequate data protection policies without prior written permission from the Texas HHS agency and comply with the Texas HHS agency conditions for safeguarding offshore Texas HHS Confidential Information.
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data MOWNCT has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases
- Allow people to request his or her own Protected Health Information (PHI), or such individual's Legally Authorized Representative, in compliance with the requirements of HIPAA.
- Restrict permissions or attempts to re-identify or further identify de-identified Texas HHS Confidential Information, or attempt to contact any Individuals whose records are contained in the Texas HHS Confidential Information, except for an Authorized Purpose, without express written authorization from a Texas HHS agency or as expressly permitted by the DUA.

Actions

To exercise data protection we're committed to:

- Annual review of policy and procedures by executive leadership and board of trustees
- Build secure networks to protect online data from cyberattacks
- Conduct staff development training on matters related to:
    - Confidentiality, privacy, and security, stressing the importance of promptly reporting any Event or Breach.
    - Attendance roster will be used to record participation along with employee's signature. One-on-one training will occur for employee unable to attend the staff development training.

- Establish data protection practices to include but not limited to:
    - Document shredding – onsite secured shred bin and crisscross paper shredder
    - Secure locks – file cabinets
    - Data encryption – email messaging
    - Frequent backups – provided by First Equipment and Accessible Solutions
    - Access authorization – limited to Authorized Users
    - Passwords – require user password changes at least every 90 calendar days; prohibit the creation of weak passwords (e.g., require a minimum of 8 characters with a combination of uppercase, lowercase, special characters, and numerals, where possible) for all computer systems that access or store Texas HHS Confidential Information
    - Clean Desk Practice:
        - PLAN
          Keep just the things needed for the workday on desk. Start each day with a few minutes of planning so that one can organize the documents needed for immediate work. File all other folders and documents.
        - PROTECT
          Secure information whenever leaving one's desk. Whether it is to attend meetings or to take breaks make a quick check to see if there is sensitive information on the desk and place it inside a folder or off the desktop. And for additional security, make sure to switch on the computer's password-protected screen saver.
        - PICK UP
          At the end of the work day do not leave documents or notes on desk. In order to maintain the security of both client and employee information, it's essential to file documents or lock them up.
- Privacy Safeguards
    - Administrative – staff development training, approval of authorized users for provision of access, termination, and review of safeguards, incident/disciplinary management, disaster recovery plans, and contract provisions.
    - Technical – protection and security of passwords, logging of client notes, emergencies, how paper is faxed or mailed, and electronic protections such as encryption of data.
    - Physical – disbursement of keys, usage of locked documents, authorized use of physical access, physical storage, and trash.
- Ensure that records retention requirements are followed including the appropriate manner of disposal of information destroyed so that it is unreadable or undecipherable.

- Non-disclosure of work done on behalf of Texas HHS pursuant to the DUA, or to publish Texas HHS Confidential Information without express prior approval of the Texas HHS agency.
- Update policies, procedures, and plans following major changes with use or disclosure of Texas HHS Confidential Information within 60 days of identification of a need for update.

Breach Notification Process:

- Contact company representative, i.e. First Equipment Accessible Solutions, Bloomerang, Texas Health and Human Services, regulatory authorities, and others as identified.
- Specifically related to Texas Health and Human Services:
    - Initial Notice of Breach will be provided in accordance with Texas HHS and DUA requirements with as much information as possible about the Event/Breach and a name and contact who will serve as the single point of contact with HHS both on and off business hours. Time frames related to Initial Notice include:
        - Within one hour of Discovery of an Event or Breach of Federal Tax Information, Social Security Administration Data, or Medicaid Client Information.
        - Within 24 hours of all other types of Texas HHS Confidential Information **48-hour Formal Notice** will be provided no later than 48 hours after Discovery for protected health information, sensitive personal information or other non-public information and will include applicable information as referenced in Section 4.01(C)2 of the Data Use Agreement.
    - No later than 5 p.m. on the third business day after Discovery, or a time within which Discovery reasonably should have been made by MOWNCT of a Breach of Confidential Information, MOWNCT shall provide written notification to HHS of all reasonably available information about the Breach, and MOWNCT's investigation,
- Activate Internal Breach Response Team
    - Determine manner/method in which to notify individuals of suspected breach
    - Work with appropriate authorities and company representatives to resolve the situation

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

Internal Breach Response Team

Incident Lead – Debbie Sheffield
Executive Director – Christine Hockin-Boyd
Information Technology - First Equipment

My signature below indicates my acceptance of the privacy & security policy.

_____
Print Name

_____ _____
Signature Date