PRIVACY POLICY

MISSION WACO MISSION WORLD, INC.

1. Purpose

This policy addresses the standards and procedures of Mission Waco, Mission World, Inc. (MWMW) when handling information about you; how it may be used and disclosed plus safeguards. This policy includes the standards for how MWMW will collect, use, and disclose the data collected for its programs, including the collection, use, and disclosure of protected personal information (PPI). This policy is to be reviewed annually, and may be amended at any time in order to reflect changes in the MWMW privacy standards.

This policy is not a contract but it shall govern all actions wherein MWMW data is the subject. A link to this policy will be made available on the MWMW website and a physical copy can be obtained by request. This policy meets the legal requirement to maintain and preserve the confidentiality of PPI.

2. Website

MWMW maintains a website as a service to our volunteers and supporters, and as a source of information for those interested in learning more about MWMW. Visitors to this site, who provide information, do so voluntarily. Visitors need not register or provide any PPI to access any part of this site.

This privacy statement demonstrates our commitment to online and offline privacy. The following formally discloses the information gathering and dissemination practices for this website.

a. WEB Site Information Collection and Use

MWMW collects only information that is voluntarily submitted. We will not share or sell information in any manner that is provided. The sole use of this information is for contact purposes—to send receipts, "Thank You" letters, and Newsletters—and to respond to questions or comments from website visitors.

b. Donations

The "Online Donations" form allows our supporters to donate conveniently via the internet. This form collects PII (Personally Identifiable Information) including contact and credit account information and stores the data in a database hosted at our web host company, Paperless Transaction Corporation http://paperlesstrans.com/index.php/about. The information stored includes the following:

- Name, address, email, and phone if provided
- Donation amount, type of card, and expiration date
- Comments and/or information related to memorial or honorarium donations

NOTE: Your complete credit card number is NOT stored in the database. The database stores a masked

form of the number that includes only the last four digits, e.g., XXXX-XXXX-XXXX-1234.
Credit account information that is collected is transmitted from our web server to Paperless Transaction Corporation where the online transaction is processed on their secure servers. This occurs when the donor clicks the "Submit" button on the "Verify Donation Information" form.

c. Information Sharing

MWMW does not share information with any person, organization, or other entity except as outlined above related to the "Online Donations" form. The sharing occurs when the "Submit" button is clicked and the data is sent to Paperless Transaction Corporation for processing.

d. Security

The website server uses Secure Sockets Layer (SSL) encryption to secure the transmission of data. This protocol applies to the "Online Donations" form and to the transmission of that data to Paperless Transaction Corporation. Data submitted via the "Feedback" form is not encrypted.
Donor information is stored within a donor management database within MWMW. Access to the database is restricted to personnel with a legitimate business need to access or modify the information contained therein.

e. Choice/Opt-Out

If anyone wants to be added or removed from our mailing list or e-news, you may:

- Send email to office@missionwaco.org requesting to be removed from the list, or click Unsubscribe in the email.
- Send postal mail to: Mission Waco/Mission World 1315 N. 15th Waco, TX 76707
- Call Mission Waco/Mission World at 254-753-4900.

f. Corrections/Update

Donors may notify MWMW of a change to information previously provided using one of the contact options noted under Choice/Opt-Out

3. Health Insurance and Clinic

PPI collected through one of our employee health insurance plans (Plan) or clinic program is protected by the HIPAA Privacy Rule. Generally, protected health information is information that identifies an individual created or received by a health care provider, health plan or an employer on behalf of a group health plan that relates to physical or mental health conditions, provision of health care, or payment for health care, whether past, present or future.

How We May Use Your Protected Health Information

Under the HIPAA Privacy Rule, we may use or disclose your protected health information for certain purposes without your permission. This section describes some of the ways we can use and disclose your protected health information.

To Business Associates*:* We may enter into contracts with entities known as Business Associates that provide services to or perform functions on behalf of the Plan. We may disclose protected health

information to Business Associates once they have agreed in writing to safeguard the protected health information. For example, we may disclose your protected health information to a Business Associate to administer claims. Business Associates are also required by law to protect protected health information.

To the Plan Sponsor*:* We may disclose protected health information to certain employees of the *Plan* for the purpose of administering the Plan. These employees will use or disclose the protected health information only as necessary to perform plan administration functions or as otherwise required by HIPAA, unless you have authorized additional disclosures. Your protected health information cannot be used for employment purposes without your specific authorization.

4. Storage and Disposal of Private or Sensitive Data

- Paper documents and electronic files will be stored in such a way as to provide two (2) levels of security. Examples: a locked filing cabinet inside a locked office or building, or a locked closet inside a locked office or building, or a password-protected computer inside a locked office or building.
- Paper documents that need to be transported between physical buildings of MWMW will be stored inside a marked clasped envelope, with the staff member couriering the documents either handing them directly to another staff member or placing them in an agreed upon locked location.
- Paper documents used to collect data will be disposed of by either micro-shredding in-house at MWMW, or through a secure third-party shredding vendor.
- Paper documents will be kept the length of time to be in compliance with any federal, state or city requirements. Typically documents will not be kept longer than eight (8) years.
- Electronic data files with regard to personal private information are stored in password protected computers as mentioned above. The computer hard drives will be wiped clean before being disposed of by MWMW.

5. HMIS-Participant Data

HUD requires unduplicated statistical demographic reports on the numbers and characteristics of clients served as well as on program outcomes. In order to address the reporting requirements mandated by HUD, the HoT has implemented an electronic management information system that will provide the necessary demographic information and reports. This system is called the Heart of Texas Homeless Management Information System (HoT HMIS). Mediware Information Systems, Inc. is the vendor of the web-based software known as ServicePoint, which was selected in 2001 as part of a competitive process. The HMIS Administrator provides training and technical assistance to users of the HoT HMIS. All Providers funded by the City of Waco's Community Development Block Grant (CDBG) or

that receive certain HUD grants are required to participate in the HoT HMIS. The only exception being domestic violence shelters which are prohibited by law from HMIS participation.
MWMW, a provider participating in the HoT HMIS, is required to collect and record certain data elements for all new and continuing clients in the HMIS weekly. Data entry should be completed weekly. All records should be up to date every Monday for clients served during the prior week. All Providers using the HoT HMIS are also required to comply with HUD's HMIS Data and Technical Standards.

a. HMIS Data Collection

A partner agency may only collect data when appropriate to provide services, to be in compliance with the law, or for a specific organizational purpose. Data must be collected by lawful and fair means at an appropriate time and location.

- A client's consent to collect the data may be inferred when a privacy notice is posted at each intake desk or a comparable location.
- In order to collect data on a third party (the client's household or emergency contacts), a written consent must be obtained from the client.

Data collected by the partner agency may include, but is not limited to, the following:

- Protected Personal Information (PPI), such as name, social security number, date of birth, gender, race, ethnicity, marital and family status, household relationships, veteran status, and disabling conditions;
- Housing information, such as address history, housing status, reason for homelessness;
- Program-specific information including, but not limited to, income, non-cash benefits, educational attainment, employment status, domestic violence experience, health status and medical information;
- Transactional information such as service need, provision, and outcome.

b. HMIS Reasons for disclosures

The prime reason we disclose your data is to provide and coordinate services between partner agencies. Disclosures are also made for some administrative purposes that relate to agency functioning and in the application for funding. In cases when data is disclosed to an agency or entity outside of the Heart of Texas Homeless Coalition, agencies will de-identify all client data, in order that no PII is passed on, except for the following reasons:

- To avoid a serious health or safety threat, if the partner agency believes that the use or disclosure of PII is necessary to prevent or lessen a serious threat to an individual or the public.
- To disclose reports of abuse, neglect or domestic violence to the proper authorities and to refer the client to the appropriate, confidential services.
- In response to a legal law enforcement request or to report a death as a result of possible criminal conduct.
- For national security and intelligence activities.
- In response to a relevant medical emergency.

- To funeral directors, coroners, and/or medical examiners, as necessary to carry out their respective responsibilities.
- In conjunction with a research project that has signed a formal agreement with the agency and the HOTHC, established rules and limitations on processing PPI within the relevant timeframe, and the unnecessary disclosure of PPI during the research process. The project must also establish a means for returning or properly disposing of all PPI at the end of the research timeframe.
- As needed to remain in compliance with local, state, and national law.

c. HMIS Privacy Rights

Clients with data in the HoT HMIS have the following rights:

- To inspect and obtain a physical copy of their data in the HMIS. The partner agency providing the copy will explain any data that the client may not understand.
- The client has the right to request a correction of any inaccurate or incomplete PPI that is present in the HoT HMIS. If the request is granted, the partner agency may delete it, amend it, or mark it as inaccurate or incomplete. If the request is denied, the client will receive a written explanation for why their request was denied. The client has the right to submit a written statement disagreeing with the agency's dissent.
- To obtain what disclosures of their PPI have been made within a set timeframe. This list does not have to include disclosures that were made for law enforcement officials, correctional facilities, national security or intelligence inquiries.
  To make a written complaint about privacy policies, practices or other security concerns. All complaints may be submitted to Mission Waco/Mission World 1315 N. 15th Waco, TX 76707.

d. HMIS Remote Access to Data

- Utilizing remote access to computers to use HoT HMIS is limited to MWMW staff who are HoT HMIS administrators, or potentially executive staff of MWMW who are approved/licensed by HoT HMIS in an emergency.