

MID AMERICA ASSISTANCE COALITION

Strengthening the social service community through information systems, training, and advocacy.

MAACLink DV VPN

Thank you for your interest in MAACLink DV VPN.

In order to become a member of the MAACLink DV VPN database system, the enclosed new agency packet must be completed. The Executive Director will need to sign the Agency Partner Agreement. In addition, all individuals requesting access to the system must complete and sign a Confidentiality Statement and Request for Account. These forms must also be signed by the Executive Director. Once the completed forms are returned, you will be contacted regarding your agency set up and scheduling the MAACLink DV VPN introductory training session.

Please call with any questions. We look forward to having you as a MAACLink DV VPN client agency.



One West Armour Blvd, Suite 301
Kansas City, MO 64111

Phone: 816-561-2727
Fax: 816-561-7277
Website: maaclink.org

FOR MAAC USE ONLY

Staff initial and date next to each item once complete

_____ Completed Agency Packet received
_____ Contact Agency regarding set up on MAACLink DV VPN
_____ Schedule MAACLink DV VPN Training (tentative date: _____)
_____ Training completed
_____ Invoice Sent

Agency Workgroups

(check all applicable)

___ EA
___ Case Mgmt
___ HMIS/APR
___ Shelter
___ Fund Manager
___ Funder
___ Hotline
___ Aggregate Only

MAACLink DV VPN

Table of Contents

Agency Information	1-2
Workgroups.....	3
General Rules	4
Agency Partner Agreement.....	5
Level 1 Privacy Agreement.....	6-7
Level 2 HMIS Privacy Agreement.....	8
Signatures.....	9

MAACLink DV VPN

Agency Information	
<i>Agency Name</i>	<i>Date</i>
<i>Does this agency have a parent agency? If so, please list the name of the parent agency.</i>	
<i>Does this agency have multiple programs and/or sites? If so, please list them.</i>	
<i>Agency Address (Physical location of agency)</i>	
<i>Billing Address (If different than agency address)</i>	
<i>Executive Director (Name, Phone, Email)</i>	
<i>Primary Contact (Name, Phone, Email)</i>	
<i>Days and hours of operation:</i>	

MAACLink DV VPN

Agency Information (Cont.)
<p><i>Is this agency a 501C3?</i></p> <p><i>If yes, please include your tax payer ID number:</i></p>
<p><i>Funding Sources</i></p>
<p><i>Do you any of your funding sources require you to enter data into an HMIS?</i> <i>If yes, please list them.</i></p>
<p><i>Total Annual Budget</i></p>
<p><i>Client Eligibility</i></p>
<p><i>Services Provided</i></p>
<p><i>Is this agency a CHO Agency? (YES OR NO)</i></p> <p><i>A CHO is “any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes Protected Personal Information (PPI) on homeless clients for an HMIS.”</i> <i>-An agency in the Continuum of Care that serves homeless clients is a CHO Agency.</i> <i>-An agency that must complete an APR for HUD is an APR Agency, and is also a CHO Agency.</i> <i>-Not all CHO Agencies must complete an APR.</i></p>
<p><i>Will this agency need to submit an APR to HUD? (YES OR NO)</i></p>
<p><i>Will this agency share data with others? (YES OR NO)</i></p>
<p><i>List the counties, towns, and/or zip codes that your agency serves</i></p>

MAACLink DV VPN

Workgroups

An agency can join any of the following workgroups (please select all that apply):

*Please keep in mind each workgroup may have an associated fee—for more information please contact the MAAC office.

Emergency Assistance (EA) Workgroup– The EA workgroup is the most basic functionality of MAACLink. The users have the ability to enter shared client and household files, services, and run related reports. This functionality also allows the case worker to record a client’s financial information and calculate the poverty level.

HMIS/APR Workgroup– For agencies that receive HUD funding and must generate Annual Progress Reports. In this workgroup the user has the HUD APR in addition to everything included in the Emergency Assistance Workgroup.

Shelter Workgroup– For agencies that have a homeless shelter. Users may enter shared client and household files, make shelter reservations, check clients in and out of the facility, add beds/rooms in a facility, maintain a restricted list, and run related reports. This workgroup also gives access to everything in the Emergency Assistance Workgroup.

MAACLink DV VPN

General Rules

MAAC's rules for using MAACLink DV VPN are designed to insure that only authorized agency staff will use the computer database for legitimate agency purposes, such as tracking client services, evaluating service needs, and creating necessary administrative reports. Unauthorized use of the system is a violation of clients' rights and a threat to the future of MAACLink DV VPN.

MAAC provides MAACLink DV VPN as a service to partner social service agencies. As stated in the contract, MAAC may withdraw the service at any time. This is the primary means of control that MAAC staff will use to deal with rules violations.

Note: This document in no way alters the agreement between MAAC and its agency partners established in the Agency Partner Agreement.

Terms and Conditions

The purpose of this document is to set out the terms under which the Mid America Assistance Coalition (MAAC) will operate MAACLink DV VPN. MAACLink DV VPN is MAAC's HMIS-compliant VPN based information system through which emergency assistance is documented, clients are tracked, funds are managed, and reporting is accomplished accurately and without duplication of effort.

The Executive Director of the MAACLink DV VPN Agency Partner must sign this agreement before an account for that agency can be established for MAACLink DV VPN.

Initials _____

MAACLink DV VPN

Agency Partner Agreement

System (MAAC) Responsibilities

MAAC agrees to assist MAACLink DV VPN participating agencies in disseminating program data pertaining to services provided to recipients. Conditions under which the exchange of information is facilitated between MAAC, MAACLink DV VPN Agency Partners, and/or other data systems will also be provided by MAAC at the request of the MAACLink DV VPN agency.

MAAC will provide initial individual or group training to agencies utilizing MAACLink DV VPN. The training may include data entry training, confidentiality training and training on how to interpret reports generated from the system. This training will be completed before a user is permitted access in MAACLink DV VPN.

MAAC agrees to do the following:

- Provide and maintain the resources necessary to support MAACLink DV VPN
- Provide necessary MAACLink DV VPN program software
- Respond to agency requests for upgrades and refinements of the software
- Provide training and technical support as requested by the participating agency

Agency Partner Responsibilities:

- The MAACLink DV VPN Agency Partner agrees to abide by all federal, state, and local laws and regulations, and with all MAAC procedures and policies relating to the collection, storage, retrieval, and dissemination of MAACLink DV VPN information
- Acquire and maintain computers and software according to MAAC standards
- Ensure that agency personnel are trained by MAAC staff before accessing MAACLink DV VPN, and that untrained and/or unauthorized personnel do not access MAACLink DV VPN.
- Assure the accuracy of information entered into the system
- The MAACLink DV VPN Agency Partner is responsible for maintaining client information updates and correcting data entry errors, and/or inaccuracies
- Follow the validation requirement for emergency assistance
- Strictly adhere to the appropriate Privacy Agreement

Errors, Negligence, or Misconduct by an Agency

If there is error, negligence or misconduct by an agency, that agency will indemnify and hold harmless MAAC, its agents, servants and employees from any and all claims, demands, actions, suits, judgments and liability arising out of or in connection with this Agreement or the use of data obtained under the terms of this Agreement.

Initials _____

MAACLink DV VPN

Level 1 Privacy Agreement

All agencies/organizations that participate in MAACLink DV VPN must adhere to the following standards:

All users must have received MAACLink DV VPN user training and have their *own* user name and password in order to access the system. Every individual, whether they are an employee or volunteer, must be an authorized user in order to gain access to MAACLink DV VPN. In order to become an authorized user of MAACLink DV VPN, each individual must complete a Statement of Confidentiality form (found on our website: maaclink.org) which must also be signed by their supervisor. Once the form is complete it must be sent to the MAAC office and training will need to be scheduled. Once the individual receives training they will then be given their unique login name and password. An authorized user cannot delegate use of their account to anyone else including other authorized users. Each authorized user must be logged in to their own account whenever they use the system in any way. Should MAACLink DV VPN participating agency administrators detect a violation of any part of the Statement of Confidentiality or the Privacy Agreement by an individual user, a Notice of Violation will immediately be given to the user agency executive director and a copy sent to the MAAC Executive Director. Any violation may be considered a breach of contract and may result in discontinuation of user or agency rights to MAACLink DV VPN.

All clients who apply for a service or program enrollment at your agency must grant informed consent to put their files into the MAACLink DV VPN system. Each agency must have their clients sign the Client Consent and Release of Information form (found on our website: maaclink.org) before their information can be entered in MAACLink DV VPN. The Client Consent and Release of Information form must be completed at least annually and stored onsite. The files entered in MAACLink DV VPN must be stored on-site for at least 7 years after the last date of service. Agencies may choose to provide additional releases of information as applicable to their individual operating procedures and policies as long as they do not conflict with the MAACLink DV VPN Client Consent and Release of Information.

An agency may obtain a verbal consent from clients as long as they have completed the Verbal Consent Agreement form and faxed or mailed it to the MAAC office. The Verbal Consent Agreement is not for each client, but instead serves as a notice to MAAC that your agency intends to collect informed verbal consent instead of signed consent from clients you serve. *Exception: Clients who receive a service from a MAAC-managed utility fund MUST sign a consent form or the Standard Intake Form that contains the consent paragraph. (See our website: maaclink.org for forms)*

Clients have a right to revoke their consent. If a client of your agency asks to have his/her file removed from MAACLink DV VPN, ask him/her to complete a Client Revocation form (found on our website: maaclink.org) for your files and call the MAAC office for guidance in removing the client's file from MAACLink DV VPN.

Clients own their MAACLink DV VPN files. Clients have the right to see their files if requested. Please keep this in mind when putting client notes, household notes or case management notes into the system.

Reports that identify clients and that are generated directly from MAACLink DV VPN should not be shared with outside individuals or organizations at any time. When submitting reports or sharing statistical information you must make sure that you are only sharing aggregate information. Anyone who is not an authorized MAACLink DV VPN user must not have access to specific client information from MAACLink DV VPN.

Sharing of client information is governed by the federal Violence Against Women Act.

Initials _____

MAACLink DV VPN

Level 1 Privacy Agreement (Cont.)

All agencies/organizations that participate in MAACLink DV VPN must adhere to the following standards:

Keep these points in mind:

Do not use information in the MAACLink DV VPN system for any unofficial interaction with the client. For instance:

1. A landlord cannot use MAACLink DV VPN to evaluate potential tenants.
2. "Friends" cannot look up information for or about their "friends".
3. Business owners or operators cannot use the system to evaluate potential employees.

Conversations about specific MAACLink DV VPN information should be kept at a professional level and such conversations should be conducted in a secure environment. When communicating (verbally or through email) with other authorized users or MAACLink DV VPN tech support please use the Client ID # to identify the client instead of other confidential client specific information.

Always log off of MAACLink DV VPN or lock your computer screen before walking away from the computer.

It is each user's responsibility to insure the privacy and security of your unique log-in information. If you suspect someone may have learned your log-in information, change your password immediately.

The MAACLink DV VPN Agency Partner shall be responsible for the maintenance, accuracy, and security of all its emergency assistance records and terminal sites and for the oversight of agency personnel regarding confidentiality.

The MAACLink DV VPN Agency Partner Executive Director must accept responsibility for the validity of all records entered by their agency and the confidential manner in which any MAACLink DV VPN information is shared. The MAACLink DV VPN Agency Partner Executive Director may designate an immediate subordinate staff member with supervisory responsibilities for verifying the accuracy of information. The MAACLink DV VPN Agency Partner will provide MAAC with the names(s) and title(s) of the staff member(s) authorized to supervise data entry personnel. The Executive Director is responsible for assigning appropriate user rights based on the job description of each staff person. These designations are made on the individual Statement of Confidentiality agreements.

Enforcement of the Confidentiality Policy

MAAC has the absolute right to terminate without notice services of MAACLink DV VPN for the purpose of investigation of any suspicion of breached confidentiality. Thereafter, MAAC may terminate this agreement if MAAC, in its sole discretion, determines that there has been a breach of confidentiality.

MAAC reserves the right to immediately suspend furnishing information covered by terms of this agreement to the MAACLink DV VPN Agency Partner when any terms of this agreement are violated or are suspected to be violated. MAAC shall resume furnishing such information upon receipt of satisfactory assurances that such violations did not occur or that such violations have been fully corrected or eliminated.

Two exceptions to the privacy agreement:

Duty to Warn—As professionals, we all have a duty to guard each other from harm. If a client has threatened you, him/herself, or others at your organization you must warn other users of a potential threat through the MAACLink DV VPN system. This may be done by placing an alert on the client's profile. This alert should be brief, clear, and factual.

Child Abuse and Neglect—If you see evidence or have reason to believe that a child/children have been abused or neglected then you have a duty to report it to authorities, regardless of confidentiality agreements. You may call 1-800-422-4453 to find a local phone number for reporting purposes.

Initials _____

MAACLink DVVPN

Level 2 HMIS Privacy Agreement

Attention: "Covered Homeless Organizations" (CHO)

A CHO is "any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes Protected Personal Information (PPI) on homeless clients for an HMIS."

Agencies and organizations that are mandated by HUD to participate in a Homeless Management Information System (HMIS) should adhere to the Level 2 privacy standards. These standards are taken directly from the Federal Register, HMIS Data and Technical Standards Final Notice, dated July 30, 2004.

Adherence to these privacy standards are the responsibility of each CHO and not up to MAAC to enforce. MAAC is providing a service to the CHO's by distributing this document. Agencies or organizations may choose to add privacy pieces into this document as applicable to their individual operating procedures and policies. The Level 2 privacy agreement is in addition to the Level 1 Basic Privacy Agreement. The Level 1 Basic Privacy Agreement **will** be enforced by MAAC and applies to all agencies.

Level 2:

CHO's must post a sign at each intake desk or comparable location that gives a general explanation of the reasons for collecting client information.

This sign is included in the privacy packet and uses HUD's specific language.

A written Privacy Notice must be available to give to clients.

Unlike this Privacy Statement you are reading, HUD specifies the creation of a Privacy Notice document that can be given directly to the client. This Privacy Notice is in addition to the consent form that clients sign before receiving service from your agency.

If a CHO maintains a public website, the current Privacy Notice must be posted on the website.

MAAC will post the HMIS privacy packet at www.maaclink.org. If your agency has a website and is a CHO, you may link to maaclink.org. If your agency chooses to use an internal privacy notice or make additions to this one, you will be responsible for posting those on your website.

The CHO must post a single sign that informs clients or potential clients about the existence and availability of the Privacy Notice.

For convenience, this notification has been amended to the intake sign that is available in this packet.

The CHO must maintain permanent documentation of all Privacy Notice amendments.

Because the Privacy Notice may vary by CHO, MAAC will not track changes or amendments to the form. This is the responsibility of each CHO. MAAC will only track changes and amendments in the Level 1 Privacy Agreement.

All staff members and volunteers at the CHO must pledge to comply with the Privacy Notice.

This compliancy will not be monitored or enforced by MAAC. MAAC will only monitor and enforce the Level 1 Privacy Agreement. It is up to each CHO to determine the best enforcement method for their respective organizations.

A CHO must install a firewall on the user's computer or the agency network.

MAAC may be able to provide some assistance or direction with this requirement. Call the office for information if your organization does not operate behind a firewall.

Initials _____

MAACLink DV VPN

Signatures	
<p><i>The Executive Director (or equivalent) of the MAACLink DV VPN Agency Partner indicates agreement with the terms stated in the MAACLink DV VPN Agency Partner Agreement and the Privacy Agreement by signing below. All pages will then be forwarded to MAAC. Both of these steps are prerequisites to the establishment of a User account on the MAACLink DV VPN program. Once received, the Executive Director of MAAC will sign this page and copies of all four pages will be sent back to the MAACLink Agency Partner.</i></p>	
Agency Executive Director Name (Please Print)	
Agency Executive Director Signature	Date
MAAC Executive Director (Please Print)	
MAAC Executive Director Signature	Date
Effective Date and Term	
<p><i>This agreement will become effective on the _____ day of _____, 20____, and continue in effect for one year.</i></p> <p><i>Thereafter, this agreement will be automatically renewed on each subsequent anniversary date, unless terminated immediately for cause or by either party with 30 days written notice.</i></p>	
Quarterly/Yearly Fee: _____	
Set up Fee: _____	