GA HMIS Interim Policies and Standard Operating Procedures

This document details the Interim policies, procedures, guidelines, and standards that govern the operations of the GA Homeless Management Information System (GA HMIS).

GA HMIS Policies and Standard Operating Procedures

Table of Contents

GA HMIS Policies and Standard Operating Procedures

GA HMIS Policies and Standard Operating Procedures

GA HMIS Policies and Standard Operating Procedures

GA HMIS Policies and Standard Operating Procedures

GA HMIS Policies and Standard Operating Procedures

GA HMIS Policies and Standard Operating Procedures

Introduction

This document details the policies, procedures, guidelines, and standards that govern the operations of the GA Homeless Management Information System (GA HMIS). It outlines the roles and responsibilities of all agencies and persons with access to GA HMIS data, and it contains important and useful information about the ways in which GA HMIS data is secured and protected. All Providers using the GA HMIS should read this document in full and train every end user within its agency and programs to understand its contents as necessary. Appendix A is a user license agreement, which includes a statement that the user has read and understands these operating procedures as per the Agency Participation Agreement.

The US Department of Housing and Urban Development (HUD), other federal and state Partners, and the GA Collaborative, also known as Continuums of Care (CoCs), require GA HMIS to provide 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 and Department of Community Affairs has implemented an electronic management information system that will provide the necessary demographic information and reports. This system is called the GA Homeless Management Information System (GA HMIS) and is administered by the GA Department of Community Affairs (DCA). All Providers funded by certain HUD as well as some providers funded locally are required to Participate in the GA HMIS, and some privately funded providers Participate on a voluntary basis.

Providers' participating in the GA HMIS are required to collect and record HUD required data elements for all new and continuing clients in the HMIS. Data entry should be completed weekly with the exception of Emergency Shelter, which should enter daily data. All Providers using the GA HMIS are also required to comply with HUD's *HMIS Data and Technical Standards* available at www.hudhre.info and on the DCA website at http://www.dca.state.ga.us/housing/specialneeds/programs/hmis.asp.

GA recognizes the importance of maintaining confidential client records in a secure environment to ensure that the information is not misused or accessed by unauthorized people. The following Policies and Standard Operating Procedures (SOP) have been developed to establish standards for the collection, storage and dissemination of confidential information by the users of the GA HMIS. GA has developed a privacy policy regarding the use and disclosure of data in the GA HMIS and by programs operated directly by GA HMIS (see Appendix C for a copy of this policy).

The GA HMIS is an "open" system which allows for the sharing of client-level data electronically between collaborating agencies, which must adhere to the GA HMIS privacy policy as well as the policies and operating procedures in this document. Agencies may also be able to share information through other methods unrelated to the GA HMIS, as outlined in their specific program policies. Data shared outside of GA HMIS is not able to be controlled or monitored by GA; therefore this data is not covered by the GA HMIS privacy policy. GA is the System Administrator for the GA HMIS and as such is the only entity with

GA HMIS Policies and Standard Operating Procedures

access to all client-level information, including personal identifiers, contained in the GA HMIS. Acceptable uses and disclosures of the data are outlined in the GA HMIS privacy policy. For example, GA may disclose data that is required under a court order issued by a judge, to protect the health and safety of those being served in its programs, and may use de-identified data for research and analysis purposes. Except in rare cases, GA does not provide access to client-level data containing personal identifiers to any non-Participating agency. Additionally, HUD does not require any client-level information from the GA HMIS for the programs it funds. Thus, only de-identified and/or aggregate-level data is shared with non-participating agencies and HUD.

GA HMIS Goals

The goals of the GA HMIS are to support and improve the delivery of homeless services in the jurisdictions it serves. Inclusive in these goals is the improvement of the knowledge base about homelessness that contributes to an enlightened and effective public response to homelessness. The GA HMIS is a tool that facilitates the following:

- *Improvements in service delivery* for clients as case Administrators assess the client's needs, inform the client about available services on site or through referral, help the client find and keep permanent housing, and improve service coordination when information is shared between programs within one agency that are serving the same client.
- *A confidential and secure environment* that protects the collection and use of all client data including personal identifiers.
- The *automatic generation of standard reports* required by HUD or other stakeholders and funders, including participation in the national Annual Homelessness Assessment Report (AHAR).
- *Generation of system-level data* and analysis of resources, service delivery needs and program outcomes for the Commonwealth's homeless population.
- A *data collection and management* tool for authorized agencies to administer and supervise their programs.

GA recognizes the need to maintain each client's confidentiality, and will treat the personal data contained within the GA HMIS with respect and care. As the guardians entrusted with this personal data, GA has both an ethical and a legal obligation to ensure that data is collected, accessed and used appropriately. Of primary concern to GA are issues of security (i.e. encryption of data traveling over the Internet, the physical security of the GA HMIS servers), and the policies governing the release of this information to the public, government and funders. Meeting the needs of homeless persons served by GA HMIS and its Providers is the underlying and most basic reason for having the GA HMIS, and employing it for continued improvements in program quality.

GA HMIS Policies and Standard Operating Procedures

Definitions

Agency Administrator: The person responsible for system administration at the agency level. This person is, or is appointed by an Agency's Executive Director.

Authorized/Particpating Agency: Any agency, organization or group who has a GA HMIS Participation Agreement and/or contract with DCA and that is allowed access to the GA HMIS Client Track application. These Agencies connect independently to the application via the Internet.

Client: shall mean any recipient of services offered by a Provider or Authorized/Participating Agency.

Client-level Data: Data collected or maintained about a specific person. This type of data can be de-identified for purposes of data analysis, which means that personally identifying information is removed from the record for reporting.

GA HMIS: The specific HMIS system utilized by the GA HMIS CoC's and other participating jurisdictions.

GA HMIS System Administrator: The job title of the person at DCA who provides oversight of GA HMIS. This person has the highest level of user access in GA HMIS and has full access to all user and administrative functions.

Database: An electronic system for organizing data so it can easily be searched and retrieved; usually organized by fields and records.

Encryption: Translation of data from plain text to a coded format. Only those with the "key" have the ability to correctly read the data. Encryption is used to protect data as it moves over the .

Firewall: A method of controlling access to a private network, to provide security of data. Firewalls can use software, hardware, or a combination of both to control access.

HMIS: Homeless Management Information System. This is a generic term for any system used to manage data about homelessness and housing.

HUD HMIS Data and Technical Standards: The initial HUD Data & Technical Standards were published July 30, 2004 Federal Register, Vol. 69, No. 146, pp. 45888 through 45934. The Department of Housing and Urban Development (HUD), the Department of Health and Human Services (HHS), and the Department of Veterans Affairs (VA) released the 2017 HMIS Data Standards on May 2, 2017. The HMIS Data Standards provide communities with baseline data collection requirements developed by HUD, HHS, and VA.

Identifying Information: Information that is unique to an individual and that may be used to identify a specific person. Examples of identifying information are name and social security number.

GA HMIS Policies and Standard Operating Procedures

Provider: Shall mean any organization within a CoC that provides outreach, shelter, housing, employment and/or social services to homeless people. For the purposes of this document, the term "provider" is synonymous with "Authorized Agency."

Server: A computer on a network that manages resources for use by other computers in the network. For example, a file server stores files that other computers (with appropriate permissions) can access. One file server can "serve" many files to many client computers. A database server stores a data file and performs database queries for client computers.

User: An individual who uses a particular software package; in this case, the GA HMIS *Client Track* software.

GA HMIS Policies and Standard Operating Procedures

Organization and Management of GA HMIS

Program Management

Policy: The Georgia Department of Community Affairs (DCA) is responsible for project management and coordination of the GA HMIS. DCA contracts with Eccovia who provides System Administration for the GA HMIS and is responsible for baseline training, system changes, reporting, custom reporting, addressing end user tickets and system change coordination. The System Administrator is the primary contact with GA HMIS Lead to implement any necessary or desired system-wide changes and updates. In this role as Project Administrator, GA endeavors to provide a uniform GA HMIS that yields the most consistent data for client management, agency reporting, and service planning.

Procedure: All concerns relating to the policies and procedures of the HMIS should be addressed with the GA HMIS Lead.

System Administration

Policy: DCA contracts with Eccovia who provides System Administration for the GA HMIS and is responsible for baseline training, system changes, reporting, custom reporting, addressing end user tickets and system coordination and administration. In the absence of the System Administrator, the backup staff member/ proxy for responding to Authorized Agencies is the DCA HMIS Coordinator.

Procedure: The GA HMIS System Administrator administers the day-to-day operations of the GA HMIS and is governed by Georgia Bylaws Code of Conduct. Among other things, this Code of Conduct governs access to the Georgia data (client level or otherwise). All system-wide questions and issues should be directed to the GA HMIS System Administrator or proxy, if System Administrator is absent. DCA HMIS Lead is ultimately responsible for all final decisions regarding planning and implementation of the GA HMIS.

Agency Administration

Policy: Each Authorized Agency must designate a staff member to be the GA HMIS Agency Administrator who is responsible on a day-to-day basis for enforcing the data and office security requirements under these Policies and Standard Operating Procedures. While one person per Authorized Agency may be designated as the Agency Administrator; a backup Administrator should be considered.

GA HMIS Policies and Standard Operating Procedures

Procedure: The Executive Director of the Authorized Agency must identify an appropriate Agency Administrator and provide that person's name and contact information to the GA HMIS System Administrator and respective CoC Administrator. Changes to that information over time should be reported immediately to the GA HMIS System Administrator respective CoC Administrator. The GA HMIS Lead is responsible for maintaining a current list of Agency Administrators.

Agency Administrators are responsible for the following:

- Serves as the primary contact between the Authorized Agency and System Admin and HMIS Lead.
- Must have a valid email address and be an active, trained user.
- Communicates the need to remove end users from the GA HMIS immediately upon termination from agency, placement on disciplinary probation, or upon any change in duties not necessitating access to GA HMIS information. All changes must be relayed to the GA HMIS System Administrator or proxy.
- Must be technically proficient with web-based software since he/she will be responsible for maintaining the Authorized Agency's GA HMIS organizational structure and information.
- Has access to all client data, user data, and agency administration information for the Authorized Agency; thus, is responsible for the quality and accuracy of this data.
- Ensures the stability of the agency connection to the Internet and *GA HMIS*, either directly or in communication with other technical professionals.
- Ensures Privacy Posting is posted and visible to all clients.
- Monitors and enforces compliance with standards of client confidentiality and ethical data collection, entry, and retrieval at the agency level.

User Access Levels

Policy: All GA HMIS Users will have a level of access to data that is appropriate to the duties of their position so that information is recorded and accessed on a "need to know" basis. All users should have the level of access that allows efficient job performance without compromising the security of the GA HMIS or the integrity of client information.

Procedure: Each CoC Representative (and/or its CoC HMIS Administrator) will identify the level of access each end user will have to the GA HMIS database. Privilege levels are detailed below:

- Manage Clients - The ability to create and edit client records and enroll clients in programs
- Manage Programs - The same privileges as "Manage clients" with the addition of the ability to edit relevant program profile information
- Manage Users - The same privileges as "Manage Programs" with the addition of the ability to manage user access and permission to programs

- Manage Agency - The same privileges as "Manage Users" with the addition of the ability to edit Agency information and create/ manage sites
- HMIS Lead – A "super user" privilege level used by the DCA HMIS Lead staff to allow "Manage Agency" access to multiple agencies (a service area).
- System Administrator - Full privileges to GA HMIS - GA HMIS System Administrator, Help Desk, and programmers only

GA Communication with Authorized Agencies

Policy: The GA HMIS Lead is responsible for relevant and timely communication with CoC Representative, who is then in turn responsible to communicate to each agency regarding the GA HMIS. The GA HMIS Lead will communicate system-wide changes and other relevant information to Agencies as needed.

Procedure: General communications from the GA HMIS Lead will be directed towards all users. Specific communications will be addressed to the person or people involved. The GA HMIS Lead will be available via email, phone, and mail. The GA HMIS email list will also be used to distribute HMIS information. While specific problem resolution may take longer, the GA HMIS System Administrator will strive to respond to Authorized Agency questions and issues within 24 hours of receipt. CoC Admins and Agency Administrators are responsible for distributing information to any additional people at their agency who may need to receive it, including, but not limited to, Executive Directors, client intake workers, and data entry staff. Agency Administrators are responsible for communication with all of their agency's users.

System Availability

Policy: GA and GA HMIS will provide a highly available database server and will inform users in advance of any planned interruption in service**.**

Explanation: A highly available database affords agencies the opportunity to plan data entry, management, and reporting according to their own internal schedules. Availability is the key element in maintaining an HMIS that is a useful tool for Authorized Agencies to use in managing programs and services.

Procedure: No computer system achieves 100% uptime. Downtime may be experienced for routine maintenance, in the event of a disaster, or due to systems failures beyond the control of GA HMIS System Administrator or the GA HMIS Lead. In the event of disaster or routine planned server downtime, the GA HMIS Lead will use Constant Contact to send correspondence that informs users of the cause and duration

of the interruption in service. The HMIS Client Track system is backed up every four hours and the entire system is backed up daily so it can be restored as quickly as possible if necessary.

Inter-Agency Data Sharing

Policy: GA HMIS is an "open" system, meaning that data can be shared between GA HMIS participating agencies. Whether data is actually shared or not is determined on a per client basis, based on user input and client data sharing preferences.

Explanation: The need for client confidentiality and the benefit of integrated case management needs to be balanced. In light of new regulations for Coordinated Entry and community needs, the privacy and security policies were designed to permit Inter-Agency data sharing while still safeguarding client confidentiality.

Procedure: When new clients are entered into GA HMIS, the initiating user must set the Client's data sharing permission (Restrict to MOU) based on the Client's response on the Release of Information form) before data sharing is permitted. These permissions control the information that is shared about the client globally.

Users must record the actual responses received by the client when setting up the client's electronic data sharing policy. Users may be monitored to ensure compliance with this policy at any time by Agency Administrators, HMIS Leads, or the GA HMIS System Administrator, in which case users will need to provide a copy of any Release of Information forms that are requested. Any user found to not adhere to the data sharing permissions allowed by the client will be immediately and permanently banned from GA HMIS, and may face possible legal action. If a user feels it is in the best interest of the client, they may further restrict the client's electronic sharing policy by setting sharing to Restrict to Org, but users may never choose to implement a less restrictive data sharing policy without collecting a new Release of Information form that has been signed by the client and permits less restrictive data sharing.

Ethical Data Use

Policy: Data contained in the GA HMIS will only be used to support or report on the delivery of homeless and housing services in Georgia. Each GA HMIS End User will affirm the principles of ethical data use and client confidentiality contained in the GA HMIS Policies and Standard Operating Procedures Manual, the GA HMIS Participation Agreement, and the GA HMIS End User Agreement. Each Authorized Agency must have a written privacy policy, including specific policies related to employee misconduct or violation of client confidentiality. All GA HMIS End Users must understand their Agency's privacy policy, and a signed policy statement must become a permanent part of the employee's personnel file.

GA HMIS Policies and Standard Operating Procedures

Procedure: All GA HMIS users will sign a GA HMIS System End User Agreement before being given access to the GA HMIS. Any individual or Authorized Agency misusing, or attempting to misuse GA HMIS data will be denied access to the database, and his/her/its relationship with the GA HMIS may be terminated. Any Authorized Agency for which the relationship with the GA HMIS is terminated will also likely be de-funded by GA and/ or the Continuum of Care in which they are located because of the statutory requirement to participate in the Continuum's HMIS.

Access to Core Database

Policy: No one but GA HMIS System Administrator/GA HMIS Lead staff will have direct access to the GA HMIS database through any means other than the GA HMIS user interface, unless explicitly given permission by GA HMIS System Administrator/GA HMIS Lead.

Procedure: GA HMIS System Administrator/GA HMIS Lead staff will monitor employ updated security methods to prevent unauthorized database access.

Client Rights and Confidentiality of Records

Policy: The GA HMIS System operates under a protocol of *inferred consent* to include client data in the GA HMIS. Each Authorized Agency is required to post a sign about their privacy policy in a place where clients may easily view it (i.e. - at the point of intake, on a clipboard for outreach providers, in a case management office). The privacy posting should include a statement about the uses and disclosures of client data as outlined in this document. Written authorization for inclusion of a client's data in GA HMIS is not required, but is inferred when a client accepts the services offered by the program and when the privacy posting is displayed for client review.

Clients may opt out of GA HMIS or be unable to provide basic personal information. Clients have the right of refusal to provide personal identifying information to the GA HMIS, except in cases where such information is required to determine program eligibility or is required by the program's funders. Such refusal or inability to produce the information shall not be a reason to deny eligibility or services to a client. When a client exercises his/her right of refusal, de-identified demographic (anonymous) information will be entered into the GA HMIS.

Each Authorized Agency shall take appropriate steps to ensure that authorized users only gain access to confidential information on a "need-to-know" basis in accordance with this document and their own Privacy Policy. Duly authorized representatives of GA may inspect client records (including electronic records) at any time, although non-GA HMIS staff will not, as a matter of routine, be permitted to access protected private information. GA and Authorized Agencies will ensure the confidentiality of all client data as described in this document.

GA HMIS Policies and Standard Operating Procedures

Explanation: The data in the GA HMIS is personal data, collected from people in a vulnerable situation. GA System Administrators, HMIS Representatives, CoC Administrators, the HMIS Lead and Authorized Agencies are ethically and legally responsible to protect the confidentiality of this information. The GA HMIS will be a confidential and secure environment protecting the collection and use of client data.

Procedure: Access to client data will be controlled using restrictive access policies. Each Authorized Agency must develop and make available a privacy policy related to client data captured in GA HMIS and through other means. A posting that summarizes the privacy policy must be placed in an area easily viewed by clients, and must also be placed on the Authorized Agency's web site (if they have one). Only individuals authorized to view or edit individual client data in accordance with the stated privacy policies and these Standard Operating Procedures will have access to that data.

Authorized Agency Grievances

Policy: Authorized Agencies will contact the GA HMIS System Administrator to resolve GA HMIS problems including but not limited to operation or policy issues. If an issue needs to be escalated, the GA HMIS System Administrator may contact GA HMIS Lead for further guidance. The GA HMIS Lead and the CoC HMIS Steering Committee, will have final decision-making authority over all grievances that arise pertaining to the use, administration, and operation of the GA HMIS.

Procedure: Users at Authorized Agencies will bring GA HMIS problems or concerns to the attention of their Agency Administrator. If problems, concerns, or grievances cannot be addressed by the Agency Administrator, the Agency Administrator will contact their respective CoC Representative, who may ask for these issues to be stated in writing. If the grievance requires further attention, the GA HMIS Lead may consult with Georgia's legal counsel. The Georgia HMIS Lead along with the GA HMIS Steering Committee shall have final decision-making authority in all matters regarding the GA HMIS.

Client Grievances

Policy: Clients must contact the Authorized Agency with which they have a grievance for resolving of GA HMIS problems. Authorized Agencies will report all GA HMIS-related client grievances to the respective CoC Representatives, who in turn, will report these grievances to the GA HMIS Lead.   If the Authorized Agency's grievance process has been followed without resolution, the Authorized Agency may escalate the grievance to the respective GA CoC Representative as outlined in the "Authorized Agency Grievances" section.

Procedure: Each Authorized Agency is responsible for answering questions, complaints, and issues from their own clients regarding the GA HMIS. Authorized Agencies will provide a copy of their privacy

GA HMIS Policies and Standard Operating Procedures

policy and/or copies of the GA HMIS Privacy Policy or GA HMIS Policies and Standard Operating Procedures upon client request. Client complaints should be handled in accordance with the Authorized Agency's internal grievance procedure, and then escalated to the appropriate CoC Representative in writing if no resolution is reached. The GA HMIS Lead is responsible for the overall use of the GA HMIS, and will respond if users or Authorized Agencies fail to follow the terms of the GA HMIS agency agreements, breach client confidentiality, or misuse client data. Authorized Agencies are obligated to report all GA HMIS-related client problems and complaints to their CoC Representative, who will determine the need for further action. Resulting actions might include further investigation of incidents, clarification or review of policies, or sanctioning of users and Agencies if users or Agencies are found to have violated standards set forth in GA HMIS Agency Agreements or the Policies and Standard Operating Procedures Manual. Upon the client's request for data removal from the GA HMIS, the Agency Administrator will delete all personal identifiers of client data within 72 hours. A record of these transactions will be kept for a period of three years by the Agency Administrator and provided to GA upon request.

Authorized Agency Hardware/Software Requirements

Policy: Authorized Agencies will provide their own computer and method of connecting to the Internet, and thus to the GA HMIS Client Track system. If possible and as funds permit, GA HMIS Lead or the respective CoC may choose to assist Authorized Agencies in obtaining computers and Internet access for the GA HMIS.

Procedure: Contact your local CoC Representative for the current status of assistance.

Hardware/Software Requirements: GA HMIS is web-enabled software; all that is required to use the database is a computer, a valid username and password, and the ability to connect to the Internet using internet browser software (Chrome, Internet Explorer, Firefox, etc.). There is no unusual hardware or additional GA HMIS-related software or software installation required. The following workstation specifications are recommended.

Minimum Workstation Requirements
- Computer: PC 500 MHz or better
- Web Browser: Google Chrome 4.0.249 or higher, Microsoft Internet Explorer 5 or higher, Mozilla Firefox 3.0 or higher, or Netscape Navigator 6.0 or higher
- Hard Drive: 2 GB
- 64 MB RAM
- Internet Connectivity (broadband or high-speed)
- SVGA monitor with 800 x 600+ resolutions
- Keyboard and Mouse

GA HMIS Policies and Standard Operating Procedures

Recommended Workstation Requirements

- ➢ Computer: 1 Gigahertz Pentium Processor PC
- ➢ Browser: Google Chrome 17.0.963 or higher, Microsoft Internet Explorer 8.0 or higher (preferred)
- ➢ 20 GB Hard Drive
- ➢ 512 MB RAM
- ➢ Broadband Internet Connection - 128 Kbps (hosted version) or LAN connection
- ➢ SVGA monitor with 800x600 + resolution
- ➢ Keyboard and mouse

Although there is no unusual hardware or additional GA HMIS-related software required to connect to the database, the speed and quality of the Internet connection and the speed of the hardware and could have a profound effect on the ease of data entry and report extraction. A high-speed Internet connection, like a DSL or ISDN line with speeds at or above 128.8 Kbps, is preferred, as is a computer with speeds above 166MHz. Google Chrome 17.0.963 or higher is the recommended platform to eliminate certain technical problems.

Authorized Agency Technical Support Assistance

Policy: GA HMIS System Administrators and the GA HMIS Lead will provide technical assistance including a help desk, training, and ongoing software support for users of the GA HMIS. Technical issues with the GA HMIS software should be addressed by submitting a ticket while logged into the Client Track system or submit an email at GAHMISSupport@dca.ga.gov. Internal hardware and internet connectivity issues should be addressed by the Authorized Agency's internal IT staff to the extent possible.

Procedure: Hardware and connectivity issues not related to the GA HMIS software are not under the control of the GA HMIS Lead or GA HMIS System Administrator and should be addressed by the Authorized Agency's internal IT staff. Authorized Agencies may send an email to GAHMISSupport@dca.ga.gov for technical support to learn what is necessary to connect to the GA HMIS Client Track system as well as to request assistance with the application itself.

Videos, Guides, Etc.

Policy: The GA System Administrators and the GA HMIS Lead will provide an array of materials to assist all GA HMIS End Users on use and functionality of the system. Each GA HMIS End User will be required to view several videos and completing an assessment prior to obtaining system access. These videos, documentation, forms, etc. will be posted in the GA HMIS webpage http://www.dca.ga.gov/housing/specialneeds/programs/hmis.asp.

GA HMIS Policies and Standard Operating Procedures

Explanation: A variety of training methods and materials targets various learning styles to provide software users with information about how the software product is used. Videos and reference guides will provide specific technical instruction to GA HMIS End Users about how to use GA HMIS Client Track.

Procedure: The GA HMIS System Administrators and GA HMIS Lead staff will create, distribute and update the necessary videos, reference guides, etc. These will include procedures that are held in common for all Authorized Agencies.

Monitoring and Evaluation

Policy: The GA HMIS Lead and participating CoCs will regularly monitor and evaluate the effectiveness of the GA HMIS Implementation and, based on the information received, will continue to make enhancements to the GA HMIS system and the Policies and Standard Operating Procedures as necessary.

Explanation: Monitoring and evaluation helps ensure security and proper usage of the GA HMIS system.

Procedure: The GA HMIS System Administrator will conduct internal system monitoring. This information will be shared with the CoCs and may be used by the CoC to monitor programs funded through the CoC as required by HUD. The HMIS Lead is authorized to conduct monitoring on behalf of the GA HMIS System Administrator and/or their CoC.

GA HMIS Policies and Standard Operating Procedures

Security and Access

User Access

Policy: Only the GA HMIS System Administrators or the GA HMIS Lead staff will be authorized to grant user access to GA HMIS. User accounts will be unique for each user and may not be exchanged or shared with other users.

Explanation: Unique user names and passwords are the most basic building block of data security. Not only is each user name assigned a specific access level, but in order to provide to clients or program management an accurate record of who has altered a client record, when it was altered, and what the changes were (called an "audit trail") it is necessary to log a user name with every change. Exchanging or sharing user names seriously compromises the security of the GA HMIS system, and *will be considered a breach of the system user agreement* and will trigger appropriate repercussions and/or sanctions for the user and agency.

Procedure: Users are not able to access any data until they are trained, all agreements are collected, and the account is activated by GA HMIS staff. The GA System Administrator and GA HMIS Lead staff will have access to the list of active end user names. Additionally, Agency Administrators will monitor the users in their agency to ensure that accounts are current.

User Changes

Policy: The Authorized Agency Administrator will notify the System Administrator and GA HMIS Lead of needed changes to the Authorized Agency user accounts. This includes revoking authorization for staff who are no longer with the agency and any needed changes to the users' agency access and privilege levels, etc.

Procedure: The Agency Administrator is required to inform the System Administrator through the ticketing system within the Client Track application of the need to revoke the user account of a terminated employee immediately upon termination of employment. For employees with user access otherwise leaving the agency, the user account should be revoked at the close of business on the person's last day of employment.

GA HMIS Policies and Standard Operating Procedures

Passwords

Policy: GA End Users will have access to the GA HMIS Client Track system via a user name and password. Passwords must be changed a minimum of once every 90 days. Users will keep passwords confidential. Under no circumstances shall a user share a password nor shall they post their password in an unsecured location; to do so *will be considered a breach of the system user agreement* and will trigger appropriate repercussions and/or sanctions for both the user and agency.

Procedure: Upon sign in with the user name and temporary password, the user will be required by the software to select a unique password that will be known only to him/her. Every 90 days, end users will be prompted to change their password. See Section entitled "User Access" for additional detail on Password security.

Password Recovery

Policy: The GA HMIS System Administrators and GA HMIS Lead staff DO NOT have access to User account passwords.

Procedure: In the event of a lost or forgotten password, the end user will use the password recovery option to reset their password. The system will ask the user for their email address, and then ask for the answer to their security question. As an extra layer of security, End Users may not choose where the password reset email is sent. Once the security question is answered correctly, an email will be sent only to the email address listed in the End User's account profile. If this account is no longer active, the End User must request assistance from the System Administrator or HMIS Lead to reactivate their account. This request must be sent to the GAHMISSupport@dca.ga.gov address. Once users receive the Password reset email which contains a temporary Password, Users must login and change their password immediately before gaining access to Agency and Client data. Each request for a new password is logged in an audit trail.

Extracted Data

Policy: GA HMIS end users will maintain the security of any client data extracted from the database and stored locally, including all data used in custom reporting. GA HMIS users will not electronically transmit any unencrypted client data across a public network. Any custom reports (electronic or printed) which are shared with non-Participating agency, must remove Client and Household names.

GA HMIS Policies and Standard Operating Procedures

Procedure: Data extracted from the database and stored locally will be stored in a secure location (not on floppy disks/CDs or other temporary storage mechanisms like flash drives or on unprotected laptop computers, for example) and will not be transmitted outside of the private local area network unless it is properly protected via encryption or by adding a file-level Password. The GA HMIS System Administrator will provide help in determining the appropriate handling of electronic files. All security questions will be addressed to the GA HMIS System Administrator via the internal ticketing system. Breach of this security policy will be considered a violation of the user agreement, which may result in personnel action and/or agency sanctions.

Data Access Computer Requirements

Policy: Users will ensure the confidentiality of client data, following all security policies in the GA HMIS Policies and Standard Operating Procedures Manual and adhering to the standards of ethical data use, regardless of the location of the connecting computer. All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer. The participating CoC may restrict access to the GA HMIS system to specific computers in the future.

Explanation: Because GA HMIS is web-enabled, software end users could conceivably connect to the database from locations other than the Authorized Agency itself, using computers other than agency-owned computers. Connecting from a non-agency location may introduce additional threats to data security, such as the ability for non-GA HMIS users to view client data on the computer screen or the introduction of a virus. If such a connection is made, the highest levels of security must be applied, and client confidentiality must still be maintained. This includes only accessing the GA HMIS via a computer that has virus protection software installed and updated.

Procedure: Each Authorized Agency and Agency Administrator is responsible for:

a) Physical space: Authorized Agencies must take reasonable steps to ensure client confidentiality when authorized users are accessing the GA HMIS system. Authorized end users are required to conduct data entry in a protected physical space to prevent unauthorized access to the computer monitor while confidential client information is accessible.
b) Use of a non-agency computer located in a public space (i.e. internet café, public library) to connect to HMIS is prohibited.
c) Time-Out Routines: Time-out (login/logout) routines on every computer to shut down access to the GA HMIS Client Track system when a computer is unattended. Time-out routines will be engaged at a minimum after 10 minutes of inactivity or at other intervals as GA HMIS Steering Committee determines.
d) Each computer that accesses GA HMIS Client Track system must have current virus software that updates automatically installed.

e) If the GA HMIS Client Track system is accessed over a network, the network must be protected by a hardware or software firewall at the server. A stand-alone machine that accesses the GA HMIS client data must also have a hardware or software firewall installed and active. This may be the firewall protection included as part of the operating system or the virus protection software installed on the computer.

Questions about security of the GA HMIS should be referred to the GA HMIS System Administrator via the internal ticketing system.

GA HMIS Policies and Standard Operating Procedures

Agency Participation Requirements

GA HMIS Agency Participation Agreements

Policy: Only Authorized Agencies will be granted access the GA HMIS Client Track system. The GA CoC's shall make the sole determination to identify Authorized Agencies that will participate in their Continuum of Care. The Executive Director of each Authorized Agency will be required to sign a "GA HMIS Agency Participation Agreement" (Appendix B) binding their organization to the GA HMIS Policies and Standard Operating Procedures and all applicable Federal, State, and local laws and regulations regarding the handling of client data before access is granted.

Procedure: Authorized Agencies will be given a copy of the GA HMIS Agency Participation Agreement, the Policies and Standard Operating Procedures Manual, and any other relevant GA HMIS paperwork prior to any end user for the agency accessing the ClientTrack system. The Executive Director should review and then signed the paperwork and return to the GA HMIS Lead. The Agency account must first be setup prior to activating an end user account under that agency.

User Accounts

Policy: In order to activate an account, an end user review and sign the GA HMIS End User Agreement and send to the GA HMIS Lead. Additionally, Agency end users will be trained to use GA HMIS Client Track system by completing the initial end user video playlist or by the System Administrator at a training sessions scheduled by the GA HMIS System Administrator or GA HMIS Lead. Once training has been completed, the end user will complete the associated training assessment and then will activate each user's account.

Sharing of accounts, User IDs, or Passwords is strictly prohibited. Users may not even share accounts, User IDs, or Passwords with management within their agency.

Procedure: Each Agency Administrator (or Executive Director) will identify the authorized users for the agency. These authorized user names should be submitted to the respective CoC in which the agency resides. The CoC Representative or CoC Admin from the CoC will notify the GA HMIS System Administrator via the internal ticket system of the need to set up new authorized end user accounts.

GA HMIS Policies and Standard Operating Procedures

GA HMIS System User Agreements

Policy: Each Authorized Agency User will sign a GA HMIS Collaborative System User Agreement before being granted access to the GA HMIS.

Explanation: Before being granted access to the GA HMIS, each user must sign a GA HMIS End User Agreement, stating that he/she will abide by the GA HMIS Policies and Standard Operating Procedures Manual, will appropriately maintain the confidentiality of client data, and will only collect, enter, and retrieve data in the GA HMIS relevant to the delivery of services to people in housing crisis.

Procedure: The CoC will distribute GA HMIS System End User Agreements to new GA HMIS Users for signature. The user will sign the GA HMIS System End User Agreement and the agreement will be faxed or emailed/scanned to the GA HMIS Lead or the System Administrator. The CoC will also file the signed GA HMIS System End User Agreements for all users. The existence of a signed GA HMIS End User Agreement for each active user will be verified in any on-site reviews or may be checked during regular monitoring of contracts. Allowing a user access to the GA HMIS system without a signed user agreement is a violation of the GA HMIS Policies and Standard Operating Procedures and may result in sanctions.

Training

Policy: The GA HMIS System Administrator and GA HMIS Lead are responsible for defining training needs and organizing training sessions for Authorized Agencies. Various training options will be provided, to the extent possible, based on the needs of GA HMIS end users. GA HMIS Client Track training materials will be provided on http://www.dca.ga.gov/housing/specialneeds/programs/hmis.asp that may be used by Agency Administrators, CoC Representatives and CoC Admins to provide extra training opportunities.

Explanation: In order for the GA HMIS to be a benefit to clients, a tool for Authorized Agencies and a guide for planners, all users must be adequately trained to collect, enter, and extract data.

Procedure: The GA HMIS System Administrator and GA HMIS Lead will provide access to training for all GA HMIS users. The GA HMIS System Administrator and GA HMIS Lead will provide support to Agency Administrators, CoC Representatives and CoC Admins, who will in turn provide for end user training above and beyond the initial training.

GA HMIS Policies and Standard Operating Procedures

Contract Termination Initiated by Authorized Agency

Policy: Authorized Agencies that are not contracted to GA HMIS may terminate the GA HMIS Agency Participation Agreement with or without cause upon 30 days written notice to GA HMIS and according to the terms specified in the GA HMIS Agency Participation Agreement. The termination of the GA HMIS Agency Participation Agreement by the Authorized Agency may affect other contractual relationships with DCA and/or requirements set forth in contracts issued by HUD. In the event of termination of the GA HMIS Agency Participation Agreement, all data entered into the GA HMIS will remain an active part of the GA HMIS system.

Explanation: While non-GA HMIS contracted Authorized Agencies may terminate relationships with DCA and the GA HMIS Collaborative, the data entered prior to that termination would remain part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in GA. The termination of the GA HMIS Agency Participation Agreement may affect other contractual relationships with DCA, HUD, or other funders.

Procedure: GA HMIS Provider Agencies are required to participate in the GA HMIS system as a condition of their funding. For all non-GA HMIS contracted Authorized Agencies terminating the GA HMIS Agency Participation Agreement, the person responsible for signing the GA HMIS Agency Participation Agreement (or a person in the same position within the agency) will notify the GA HMIS System Administrator 30 days or more prior to the date of termination. In all cases of termination of GA HMIS Agency Participation Agreement, the GA HMIS System Administrator will disable all user accounts from that Authorized Agency on the date of termination of agreement.

Contract Termination Initiated by GA

Policy: DCA may terminate the GA HMIS Agency Participation Agreement for non-compliance with the terms of the agreement or with the GA HMIS Standard Operating Procedures with written notice to the Authorized Agency. DCA may also terminate the GA HMIS Agency Participation Agreement with or without cause with 30 days written notice to the Authorized Agency and according to the terms specified in the GA HMIS Agency Participation Agreement. If a GA HMIS contract is terminated under the terms of that contract, the GA HMIS Agency Participation Agreement(s) for GA HMIS access for that/those Agency(ies) will also be terminated. In that case, access may be renegotiated by DCA and the agency if appropriate and in accordance with these standard operating procedures. The termination of the GA HMIS Agency Participation Agreement or contract with DCA may affect other contractual relationships with GA, HUD, or other funders. In the event of termination of the GA HMIS Agency Participation Agreement or GA HMIS contract, all data entered into the GA HMIS will remain a part of the GA HMIS. If termination of the GA HMIS Agency Participation Agreement or GA HMIS contract occurs, all Authorized Agency end user

GA HMIS Policies and Standard Operating Procedures

accounts will be disabled on the date the GA HMIS Agency Participation Agreement or contract is terminated.

Explanation: While DCA may terminate the GA HMIS Agency Participation Agreement or its contract with the Authorized Agency, the data entered by that Authorized Agency prior to termination of contract would remain part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in GA. The termination of the GA HMIS Agency Participation Agreement may affect other contractual relationships with GA, HUD, or other funders.

Procedure: GA HMIS Provider Agencies are required to participate in the GA HMIS as a condition of their funding. Willful neglect or disregard of the Standard Operating Procedures will result in immediate termination of an Authorized Agency from the GA HMIS. If a contract with an authorized agency or collaborative of authorized agencies is terminated, that/those Agency(ies) will be terminated from GA HMIS. For all non-GA HMIS contracted Authorized Agencies for which the GA HMIS Agency Participation Agreement is terminated, the GA HMIS System Administrator will notify the CoC Representative 30 days or more from the date of termination. The CoC will notify the Provider Agency. In all cases of termination of GA HMIS Agency Participation Agreement, the GA HMIS System Administrator will disable all user accounts from that Provider Agency on the date of termination of agreement.

GA HMIS Policies and Standard Operating Procedures

Data Collection, Quality Assurance and Reporting

Required Data Collection

Policy: Authorized Agencies funded by HUD (either through DCA or directly) through the Supportive Housing Program, Shelter Plus Care, HOPWA, Section 8 Moderate Rehabilitation, the Emergency Shelter Grant, the Homelessness Prevention and Rapid Rehousing Program, or Emergency Solutions Grant are required to participate in HMIS by HUD. Other providers contracted by other State or Federal departments may also be required to participate in the GA HMIS. All Authorized Agencies that participate in HMIS are considered "Covered Homeless Organizations" (CHO) and are required to comply with HUD's *HMIS Data and Technical Standards* unless those standards are in conflict with local laws. This includes the collection of required data elements.

Authorized Agencies shall collect and enter all HUD required data elements on every client served by the Provider upon intake into the Provider's facility or program. Authorized Agencies may choose to collect more client information for their own case management and planning purposes or to comply with requirements from their CoC or funders.

Timeliness of Data Entry: Providers are required to enter basic client intake data into the GA HMIS weekly. Emergency Shelter programs must complete all data entry within 24 hours of a client being served which includes their entry or exit from their Program.

Procedure: Each agency should review and enter all HUD required data into GA HMIS as specified by HUD per Program Type.

Client Consent

Policy: Each agency must post a sign at each intake or comparable location and on its web site (if applicable) explaining the reasons for data collection for those seeking services. Consent for entering of data into GA HMIS may be inferred when the proper privacy notice is posted and if the client accepts the services offered. If a client chooses to not share their data through GA HMIS, all of the client's data may still be collected and stored in GA HMIS, but data sharing must be disabled for that client's record (i.e. "locked").

GA HMIS Policies and Standard Operating Procedures

Explanation: Privacy Policies should be in effect for each agency to both inform clients about the uses and disclosures of their personal data and to protect the agency by establishing standard practices for the use and disclosure of data. Each client must give permission for the disclosure and/or use of any client data outside of the privacy policy developed and posted by the agency. Client consent notices must contain enough detail so that the client may make an informed decision. Clients may withdraw permission to have their personal protected information in the HMIS, or may make a request to see copies of his or her client record.

Procedure: Authorized Agencies will develop a privacy posting, which will be posted in appropriate areas for client review.

Client Consent Forms for Data Sharing

Policy: GA HMIS participating/authorized agencies must use the GA HMIS Client Consent to Share form to collect all clients' sharing consent (Appendix F). Each agency should include in its privacy policy that data collected by the agency is disclosed to the DCA HMIS Lead as part of its administrative responsibility for the GA HMIS and that the data may be used for analysis and reporting purposes. DCA HMIS Lead will only report aggregate and/or de-identified data as part of its responsibilities, and agrees to maintain the data with the highest level of confidentiality and within the security guidelines set forth in this document.

Procedure: Each client must have a signed GA HMIS Client Consent to Share form on file which records their permission (or lack thereof) before users can share their data via GA HMIS.

Appropriate Data Collection

Policy: GA HMIS end users will only collect client data relevant to the delivery of services to people in housing crises as required by HUD and/or required by funders or by law.

Explanation: The purpose of the GA HMIS is to support the delivery of homeless and housing services in Georgia. The database should not be used to collect or track information not related to serving people in housing crises or otherwise required for policy development, planning, or intake purposes.

Procedure: Agency Administrators will ask the GA HMIS System Administrator for any necessary clarification of appropriate data collection. The GA HMIS System Administrator, in consultation with GA HMIS Steering Committee, will make decisions about the appropriateness of data being entered into the

database. The GA HMIS Lead may periodically audit an agency's data collection practices to ensure the database is being used appropriately.

Ownership

Policy: The GA HMIS, including any and all data stored in the GA HMIS, is the property of the DCA. DCA has authority over the creation, maintenance, and security of the GA HMIS. Violations of the GA HMIS Agency Participation Agreement, the Standard Operating Procedures, and Privacy Policies may be subject to discipline and/or termination of access to the GA HMIS.

Procedure: The GA HMIS Agency Participation Agreement includes terms regarding the maintenance of the confidentiality of client information, an acknowledgement of receipt of the Policies and Standard Operating Procedures Manual, and an agreement to abide by all policies and procedures related to the GA HMIS including all security provisions contained therein. Because programs participating in the GA HMIS are funded through different streams with different requirements, DCA shall maintain ownership of the database in its entirety in order that these funders cannot access data to which they are not legally entitled.

Data Entry - Client Profile Sharing Level

Policy: Users will accurately record the real time data sharing level(s) indicated by the client. Repeated violation of this policy may lead to personnel action and or action against the Authorized Agency, including but not limited to immediate termination of user and/or agency access.

Procedure: Client information will not ever be shared unless the user expressly sets up a data sharing policy in the client's profile. It is imperative that, once a data sharing policy is set up for a client, users at an Authorized Agency keep this information current, modifying a current policy record or creating a new policy record as necessary, in accordance with changes to the client's GA HMIS Client Consent to Share form.

Additional Customization

Policy: Authorized Agencies may request additional desired customization (such as special reports) directly from the respective CoC Representative. Agency or CoC level customizations will be considered

by the GA HMIS Steering Committee on a case-by-case basis. If the customization requires development by Eccovia, billing will be set up based upon a contract between the Authorized Agency(ies)/CoC and GA.

Explanation: It is the responsibility of individual Agencies to determine the best way to use GA HMIS for internal data collection, tracking, and reporting. This may include purchasing additional customization.

Procedure: Authorized Agencies will contact their CoC Representative in order to discuss additional customization needs.

Data Integrity

Policy: GA HMIS users will be responsible for the accuracy of their data entry. Authorized Agency leadership will be responsible for ensuring that data entry by users is being conducted in a timely manner and will also ensure the accuracy of the data entered. Data may also be used to measure program efficacy, which impacts funding opportunities during competitive funding processes such as the annual Continuum of Care application to HUD or annual ESG applications.

Procedure: It is the responsibility of each Authorized Agency to monitor the quality and accuracy of its GA HMIS data, not the GA HMIS Lead. However, the GA HMIS Lead may periodically audit data integrity. In order to test the integrity of the data contained in the GA HMIS, the GA HMIS System Administrator will perform periodic data integrity checks on the GA HMIS. The data integrity checks will include reporting of "overlaps," possible verification of data and comparison to hard files, as well as querying for internal data consistency and null values. Any patterns of error will be reported to the GA HMIS Lead and the GA HMIS Steering Committee. When patterns of error have been discovered, users will be required to make corrections where possible, correct data entry techniques, and improve the accuracy of their data entry.

Quality Control: Data Integrity Expectations

Policy: Accurate and consistent data entry is essential to ensuring the usefulness of the GA HMIS. Authorized Agencies will provide acceptable levels of timeliness and accuracy. Authorized Agencies without acceptable levels of data quality or timeliness may have payments withheld or incur other contract sanctions until the problems are addressed.

Procedure: The Continuum of Care, will perform data integrity checks on its respective GA HMIS authorized agencies.

GA HMIS Policies and Standard Operating Procedures

On-Site Review

Policy: The DCA Lead may perform reviews of an Authorized Agency's procedures related to the GA HMIS as part of monitoring. Additional monitoring may take place by funding bodies, or CoCs.

Procedure: Reviews enable the GA HMISs Lead and the CoCs to monitor compliance with the Policies and Standard Operating Procedures Manual and GA HMIS Agency Participation Agreements. The exact procedures for on-site reviews will be determined in advance of the actual on-site review.

Client Data Retrieval

Policy: Any client may request to view, or obtain a printed copy of, his or her own records contained in the GA HMIS. This information should be made available to clients within a reasonable time frame of the request. No client shall have access to another client's records in the GA HMIS.

Procedure: A client may ask his/her case Administrator or other agency staff to see his or her own record. The case Administrator, or any available staff person with GA HMIS access, will verify the client's identity and print all requested information. The client may request changes to the record, The agency can follow applicable law regarding whether to change information based on the client's request. A log of all such requests and their outcomes should be kept on file in the client's record.

Public Data Retrieval

Policy: The GA HMIS Lead will address all requests for data from entities other than Authorized Agencies or clients. No individual client data will be provided to any group or individual that is neither the Authorized Agency that entered the data or the client him or herself without proper authorization or consent.

Procedure: All requests for data from anyone other than an Authorized Agency or a client must be directed solely to GA HMIS Lead. GA may also issue periodic public reports about homelessness and housing issues in the areas covered by GA HMIS. No individually identifiable client data will be reported in any of these documents.

GA HMIS Policies and Standard Operating Procedures

Data Retrieval Support/Reporting

Policy: Authorized CoC HMIS Administrators will create and run CoC- level and agency-level reports.

Explanation: Authorized CoC HMIS Administrators and the System Administrators have the ability to create and execute reports on CoC –wide and agency-wide data, depending on their privilege level. This allows Authorized CoC HMIS Administrators to support CoC-level and agency-level goals.

Procedure: The CoC HMIS Administrators will be trained in the use of reporting tools by the System Administrator. The System Administrator will provide query functionality and templates for reports specifically for GA HMIS. The System Administrator may assist with the development of or running of reports/queries.

GA HMIS Policies and Standard Operating Procedures

DATA SHARING & SECURITY

- Clients are uniquely identified by a database-managed identity field.
- GA HMIS maintains the following:
  a. User permissions are assigned by role and by Agency/Site
  b. Users are logged out of the system after a configurable period of inactivity (20 minutes)
  c. Passwords must be changed periodically (90 days)
  d. Inactive end users must contact the System Administrator to re-activate the end user account.
- GA HMIS uses HTTPS/SSL Standards for data transmission.
- Passwords must be updated every 90 days, and cannot be reused.

DISASTER RECOVERY

- Disaster recovery for the GA HMIS application is managed by Eccovia.
- A full back up of the Database is performed nightly. Incremental and Transactional backups are done periodically during the day. All back up files are moved off site.

GA HMIS Policies and Standard Operating Procedures

Appendix A: GA HMIS End User Participation Agreement

GA HMIS Policies and Standard Operating Procedures

Appendix B: GA HMIS Agency Participation Agreement

GA HMIS Policies and Standard Operating Procedures

Appendix C: GA HMIS Privacy Policy

GA HMIS Policies and Standard Operating Procedures

Appendix D: GA HMIS Client Consent Form