Bridging the Gap

HMIS Policies and Procedures Manual

July 2022

Table of Contents

I. Overview and HMIS Documents

A. Background

The Homeless Management Information System (HMIS) is designed to capture client and services data on the characteristics and needs of homeless and at-risk individuals. In response to a congressional directive, the Department of Housing and Urban Development (HUD) has required that all CoCs implement an HMIS. This HMIS policy and procedures manual guides the implementation of the HMIS for Bridging the Gap Continuum of Care (BTG), which encompasses the rural counties of Kauai, Maui, and Hawaii.

HMIS data allows BTG to better understand the scope of homelessness locally and to allocate resources more effectively. The HMIS directly benefits service providers and homeless clients by providing more efficient and coordinated services. The HMIS is a valuable resource because of its capacity to integrate and deduplicate data from providers that enter data into the system. Aggregate HMIS data can be used to better understand the size, characteristics, and needs of the homeless population at the local, state, and national levels. The HMIS enables organizations that operate homeless assistance, prevention, and diversion programs to improve services by collecting and analyzing data about the clients they serve. The HMIS provides real-time access to housing resources and referrals and helps BTG to manage its Coordinated Entry System (CES) operations more efficiently.

The HMIS Lead is designated by BTG to administer the HMIS. Since inception in 2004, the HMIS has grown into a robust data collection and reporting tool utilized by many homeless service providers across the Neighbor Islands.

B. HUD HMIS Data Standards

HMIS Data Standards have been established by HUD to standardize data collection for homeless individuals and families receiving homeless services. The HMIS Data Standards provides the framework for data collection and reporting efforts of HMIS Lead Agencies, CoCs, HMIS Lead Agencies, HMIS System Administrators, and HMIS Users to help them understand the data elements that are required in an HMIS to meet participation and reporting requirements established by HUD and the federal partners. Resources and information on the current HMIS Data Standards can be found here: HUD HMIS Data Standards.

C. Annual Homeless Assessment Report (AHAR)

The Annual Homeless Assessment Report (AHAR) is a HUD report to the U.S. Congress that provides nationwide estimates of homelessness, including information about the demographic characteristics of homeless persons, service use patterns, and the capacity to house homeless persons. The report provides statistics on persons who experience homelessness during the year, point-in-time counts of people experiencing homelessness, and data about the inventory of shelter and housing available in a community.

The AHAR aggregates key findings from CoC's Point-In-Time Count (PIT) and Housing Inventory Count (HIC) reporting conducted during the last ten days of January. The AHAR provides national, state, and CoC-level PIT and HIC estimates of homelessness, as well as estimates of chronically homeless persons, homeless veterans, and homeless children and youth. The HUD AHAR Reports page provides more information and resources.

D. Longitudinal Systems Analysis (LSA)

The McKinney-Vento Homeless Assistance Act as amended by the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009 views the local homeless response as a coordinated system of interconnected service options as opposed to homeless assistance programs and funding sources that operate independently in a community. The LSA uses HMIS data to communicate critical information about how people experiencing homelessness use BTG's system of care. The HUD LSA page provides tools and guidance in support of this important report. The **Reports | System Performance | LSA** section of the BTG website displays annual LSA reports that convey information about BTG's system of care.

E. HUD System Performance Measures (SPM)

The HEARTH Act requires BTG to measure its performance as a coordinated system and established a set of performance measures that HUD uses to evaluate system performance. These measures encourage CoCs to regularly evaluate progress in meeting the needs of people experiencing homelessness in their community and to align programs with these principles. The six measures HUD evaluates are listed below along with a brief description of each. HUD uses SPM data as part of its CoC Program funding process each year. BTG uses this data to improve its homeless services system.

- ✓ **Measure 1:** Length of time persons remain homeless
- ✓ **Measure 2:** Returns to homelessness of those exiting to permanent housing (recidivism)
- ✓ **Measure 3:** Point-in-time count data and annual shelter service counts
- ✓ **Measure 4:** Employment and income growth for adult leavers and stayers in CoC Program funded projects
- ✓ **Measure 5:** Persons homeless for the first time within the last two years
- ✓ **Measure 7:** Successful placements from street outreach projects, exits to permanent housing, and permanent housing retention

BTG plays an integral role in the Consolidated Plan process each year and provides the Emergency Solutions Grant (ESG) Recipient with information and data necessary to complete the Con Plan for homeless assistance. HMIS and SPM data specific to ESG-funded projects are an essential part of this process.

Federal SPM resources can be found here. The **Reports | System Performance** section of the BTG website compiles the BTG SPM that have been submitted to HUD since inception in FY 2015 along with rural county comparisons since FY 2018.

F. HMIS Organization and Management

HMIS Lead: The HMIS Lead oversees BTG's HMIS operations and is responsible for administering HMIS funds in accordance with eligible activities and specifications outlined in the HMIS Lead MOA with BTG. The MOA can be found in BTG's Governance Charter, under the About BTG section of BTG's website. This section contains information on the current Board of Directors, HMIS Admin Team, and BTG Organizational Structure. The HMIS Lead provides services including but not limited to the following:

- System configuration and customizations
- Data quality assessments
- Compliance reporting to federal stakeholders
- Custom reports development
- Data analysis and ad hoc report requests
- Monitoring and evaluation
- In-person and online user training
- Technical support to HMIS contributing organizations
- Communication with the HMIS vendor
- Coordination with community partners and stakeholders

HMIS/Data Committee: BTG's HMIS/Data committee is comprised of homeless services agencies and board members that frequently utilize the HMIS. Committee responsibilities include but are not limited to the following.

- Soliciting feedback from end users and the BTG BOD
- Using feedback to develop and improve HMIS functionality
- Reviewing formal written HMIS Policies and Procedures annually
- Monitoring and improving data quality for HMIS contributing organizations
- Collaborating with other BTG committees and community stakeholders
- Making recommendations to the BTG BOD related to HMIS operations
- Providing input related to data sharing requests from non-contributing HMIS organizations
- Providing input related to ad hoc data requests

HMIS Contributing Organizations and Users: Agencies must complete the HMIS Participation Agreement, read through the HMIS Policies and Procedures, complete required documents, and attend training on how to use the HMIS before access is granted. Training information can be found on the BTG website under HMIS Support. For established HMIS organizations, new users must fill out the BTG New User Agreement and Training Request Form. This form is then submitted to the HMIS admin personnel who will issue login credentials once prerequisite requirements have been satisfactorily completed. New organizations must be approved by the BTG BOD and should reach out to their local chapter chair. Current chair information can be found on the BTG website. The HMIS Lead has also developed training materials that are contained within the system once users are granted access. Agencies may request ad hoc training from the HMIS Lead as needed.

HMIS Support: HMIS-related issues and questions should be directed to the admin team through the HMIS Helpdesk. New users must create an account prior to submitting questions as part of this process. Information on how to setup an account, as well as background on the ticket system can be found under the HMIS Support section of the BTG website. The admin team provides updates on enhancements to the HMIS through HMIS Listserv. Please contact the HMIS Helpdesk if you would like to be added to the HMIS Listserv.

G. Domestic Violence Organizations

Per HUD guidelines, domestic violence agencies must not enter any personally identifying information into the HMIS. Specifically, HUD's confidentiality provisions direct victim service providers not to disclose, for the purposes of HMIS, personally identifying information about any client. In accordance with this statutory requirement, victim service providers must maintain the confidentiality of these clients. If domestic violence agencies receive CoC Program or ESG funding they must enter applicable client and service data into an HMIS comparable database that adheres to the latest HMIS Data Standards.

H. BTG Custom Data or Report Request Form

This form can be accessed through the **Forms | HMIS Admin** section of the BTG website and should be used to request ad hoc analysis or to develop new custom reports or dashboards. Before a request is made, please review the reports page of the website and the set of existing reports that are currently available in the system. The HMIS contains an extensive collection of reports and dashboards that may already meet your needs. All requests are subject to review by the HMIS Lead and the BTG BOD to assess complexity, feasibility, and to ensure that BTG's privacy standards are upheld. Approval of data requests and applicable fees will be determined by the BTG BOD.

I. BTG HMIS New User Agreement and Training Request Form

This form can be accessed through the **Forms | HMIS Admin** section of the BTG website. BTG organizations can obtain access to the HMIS by submitting the New User Agreement and Training Request forms through the HMIS Help Desk. BTG is mindful of protecting the personal protected information of individuals entered in the HMIS. New users must sign the Statement of Confidentiality and agree to comply with all confidentiality requirements. In addition, training must be completed before access to the HMIS is granted. New users must also submit the BTG Training Request Form to schedule a training session.

J. BTG Client Informed Consent and Authorized Agency List

These forms can be accessed through the **Forms | HMIS Admin** section of the BTG website. Confidentiality and informed client consent are integral to the data collection process. The Client Informed Consent form and BTG Authorized Agency List support confidentiality and security standards to protect and inform the client as to how their data will be used.

K. BTG HMIS Participation Agreement

This agreement can be accessed through the **About BTG | Policies & Procedures** section of the BTG website. The agreement addresses the respective roles and responsibilities of HMIS Lead and Partner Agency for ongoing HMIS service and activities. The specific responsibilities of the parties to this agreement for the confidentiality, reporting requirements, training, policies and procedures, hardware, and software for the HMIS are clearly defined within to ensure that BTG maintains an effective, efficient, and secure system. All documents and addendums referenced in the agreement are also part of the agreement. HMIS Lead will abide by all applicable laws, and the Partner Agency will be expected to do the same. This document should only be completed and submitted to the HMIS Lead after the BTG BOD has formally approved the organization's HMIS access.

II. HMIS Data Quality

A. Overview and Purpose

Data Quality refers to the reliability and validity of client and services data collected by project staff and entered in the HMIS. **Reliability** refers to the degree to which the data are complete (e.g., all questions answered with valid and useable responses) and consistent (results can be duplicated within and across different sites collecting data using the same instruments). **Validity** measures the degree to which data are accurate and represent the true measure of the concept.

Reliable and valid HMIS data:
1. Allows BTG to better understand the characteristics of persons experiencing or at-risk of homelessness and how these characteristics change over time
2. Conveys accurate information about clients who utilize the homeless services system
3. Enables consistent, dependable evaluation of performance
4. Provides empirical data that can be used as the basis of new program interventions

B. Improving HMIS Data Quality

The sections that follow set expectations, procedures, and benchmarks that will improve data quality in five key areas for the purposes of analysis, reporting, planning, and coordination. Improving data quality will enhance BTG's ability to achieve statistically reliable, accurate and complete data. Annual updates to this manual should be targeted to reflect changes to the Data Standards, data entry procedures, stakeholder needs, strategic initiatives, and enhancements to performance plans.

1. Fidelity to Data Entry Protocols

Maintaining rigorous data collection standards ensures that the HMIS can provide accurate reporting. An important area includes procedures relating to the collection of discharge data. Since a formal client discharge interview is not always possible, it becomes important that client data are maintained in case files. BTG should strive for direct entry of project enrollment and exit interviews in the HMIS. Also important is the collection of data using the most current hardcopy forms, which are available on the BTG website.

2. Improving Data Entry Timeliness

Entering data in the HMIS at project entry or soon after the enrollment has been completed has several benefits.

a. Ensures that program utilization reporting reflects actual occupancy relative to program capacity.
b. Improves data quality by reducing recollection errors (which increase as time between collection and data entry lapses).
c. Enables accurate real-time service utilization reporting. Data is critical to BTG strategic planning activities for addressing homelessness.

The following table outlines data timeliness benchmarks by project type for various data collection points. For homeless street outreach projects data quality is not evaluated until a date of engagement has been entered in the system for each enrollment. This allows outreach providers time to develop rapport with the client before being held accountable to data quality standards. Once a date of engagement is established, providers are expected to collect all applicable universal and project specific data elements for their projects within the acceptable error rates presented below. Street outreach projects should coordinate their efforts and work towards reducing the number of clients without a date of engagement.

Data Timeliness Benchmarks

Project Type	Benchmark & Collection Points
Support Services Only (SSO)	72 hours from project entry, update, exit, encounter
Street Outreach (SO)	72 hours from project entry, update, exit, encounter
Emergency Shelter (ES)	72 hours from project entry, update, exit
Transitional Housing (TH)	72 hours from project entry, update, exit
Permanent Housing (PH)	72 hours from project entry, update, exit
Homelessness Prevention (HP)	72 hours from project entry, update, exit

3. Reducing Client and Enrollment Duplication

Using search criteria effectively in the HMIS before enrolling clients is the most important method for reducing client duplication in the system. Before enrolling a new client it is important that users search to determine if the client has been entered in the HMIS at some point previously.

Limiting the search to the last name field is an effective way to search for clients in the database. Searching for a client using more than one field and using a client's full identifying info increases the likelihood that a matching client will not be identified and that a new client will be created that already exists. If you suspect that a client has already been entered into the HMIS at some point and the client has a difficult last name, you may want to search using wildcard characters (*).

As an example, Hakeem Olajuwon could be searched for by using the following method:

1. If you are certain that the first three letters of the last name are correct, you could type **"Ola*"** in the last name field.
2. This will bring up all clients in the database with last name starting with "Ola".
3. If you wanted to narrow the search results you could type Ha* in the first name field and Ola* in the last name field.

Generally, simple last or first names will bring up the desired client with no problem. However, it is still recommended to use the above approach when searching as some common names return many results. It is recommended that the SSN or alias fields be used with great care. Searching only by SSN increases the likelihood of error due to transposition errors. The HMIS contains many client records and every search for a client should be conducted with the assumption that

the client already exists. A new client record should be created only after exhausting all recommended search strategies and having used at least three search methods independently.

Deleting Duplicate Enrollments
HMIS users must ensure that duplicate enrollments are not created that represent the same entry information. When duplicate enrollments are identified in the HMIS, the agency user should delete the enrollment(s) that are in error after ensuring that the most accurate record is retained.

4. Improving and Measuring Data Completeness

Data entered in the HMIS must be complete. Missing data leads to inaccurate reporting, affects service provision, and can impact funding decisions. BTG's goal is to collect complete data for all clients served, however, at times this is not possible or realistic. BTG has established acceptable rates for unknown, refused, and data not collected values. The table below establishes these thresholds. Required data elements in the system vary based on project type and funding source, as outlined in the HUD Data Dictionary.

BTG Data Completeness Thresholds

Data Element Type	Applicable Project Types	Acceptable Error Rate for Each Data Element
Universal	Support Services Only Street Outreach Emergency Shelter Transitional Housing Permanent Housing Homelessness Prevention	<=5%
Program Specific	Support Services Only Street Outreach Emergency Shelter Transitional Housing Permanent Housing Homelessness Prevention	<=5%

Data quality reports are available in the system under the Agency Admin role. Running a data quality report in the HMIS is straightforward and will identify error rates for all the data elements listed in the report. Hyperlinks display within the main report, which link to sub-reports highlighting the clients and enrollments with unknown, refused, and data not collected values. Please refer to training resources or submit a Helpdesk ticket if further assistance is needed. As a reminder, programs should not enter "0" in the SSN field.

5. Data Accuracy and Consistency

Information entered in the HMIS must reflect actual information for the client being served as of the data collection point. Recording information in the HMIS that is known to be false is strictly prohibited. Data must be collected and entered in a consistent manner, while adhering to timeliness and completeness standards. Data entry staff must have separate passwords and

complete initial training with the HMIS Lead before entering client data. **The HMIS Lead must be notified immediately if agency HMIS staff resign or are terminated.**

Several strategies are suggested below for street outreach data collection.

1. Clients declining HMIS consent can be entered in the HMIS, however, this information cannot be shared with other organizations. Providers should work to build trust with the client while in the project to obtain consent, which can then be easily updated in the system.
2. A date of engagement should not be established for a street outreach project enrollment until the client can be engaged in housing related services and has agreed to provide all required assessment data pertaining to the street outreach project. This includes discharge data.
3. If a date of engagement cannot be obtained initially, client demographic and personally identifying information should be collected to the best extent possible, including accurate name information. This information should then be entered in the system as the foundation for the enrollment. As rapport and trust are established with the client and a date of engagement can be established, the client should be marked as engaged in system, and remaining assessment data updated.
4. Clients with a date of engagement should never auto-exit, as this negatively impacts BTG system performance. To prevent auto-exit, an encounter must be recorded in the system for the head of household at least once every 90 days.

Sampling of client files will be performed during periodic monitoring by the HMIS Lead. Staff will request a sample of the client's hardcopy HMIS forms and compare these hardcopy files to information entered in the HMIS. If HMIS records differ, corrective action will be needed.

Data consistency checks will be used to monitor HMIS data to ensure that the following types of inconsistencies are not occurring within the data.

- Overlapping project entry and exit dates for the same client over multiple enrollments for project types where this should not be occurring.
- A client that is missing project exit data from one shelter project while active in another shelter project.
- A client with duplicate active enrollments within the same project.

Often, running an unduplicated or duplicated report and sorting by client last name can identify inconsistencies in project data. If identified, duplicate enrollments should be deleted by agency users. Multiple client IDs representing the same person should be merged by contacting the HMIS Lead.

C. Updating Data During the Program Stay

While the bulk of client information entered in the HMIS is collected during the project entry and exit interviews, the HMIS must be updated to reflect changes to project entry data for some data elements that occur while the client is active in the project. Disability, income, benefits, and health insurance domains are both difficult to collect at project entry interview and may change while the client is active in the project. Please refer to HMIS training materials or reach out to the HMIS Helpdesk on how to complete during or annual assessments in the system.

D. Data Monitoring Responsibilities and Compliance

HMIS contributing organizations must remain in compliance with the documents, policies and procedures presented in this manual and partner with HMIS Lead staff to quickly and accurately remedy data or procedures that do not meet compliance thresholds. It is the responsibility of BTG to implement effective improvement and enforcement policies to support the monitoring and improvement process.

The HMIS Lead will run monthly monitoring reports and post results to the Reports section of the BTG website by the fourth week of the following month. The HMIS Lead will review the reports and follow up with organizations as necessary to rectify data quality issues. It is the provider's responsibility to review the reports and bring discrepancies to the attention of the HMIS Lead. Random census listings for active HMIS projects may be requested to determine if clients have been entered within the standards set forth. Agencies not meeting standards will be asked to provide an explanation and resolve any findings. Repeated findings or inability to address issues may be presented to the BTG BOD or funder to assist with a resolution.

The HMIS Lead will measure completeness by running organizational data quality reports for comparison against stated thresholds. Every agency will be monitored at least once within a two-year cycle. Summary reports and findings will be sent to provider staff. Providers will be required to provide explanations and improve data quality within stated timeframes. Failure to correct findings may be presented to the BTG BOD or funder to assist with a resolution.

E. Relating HMIS Data to the Housing Inventory Count (HIC)

Monthly census reporting is displayed under the **Reports | Monitoring Reports** section of the BTG website and compares active client and household HMIS data as of the end of each month for ES, TH, and PSH project types to project capacity data from the most recent HIC. The most recent HIC can be accessed in Excel format from the **Reports | HIC & PIT** section of the BTG website and aligns with the most recent point-in-time count date. The difference between HIC Beds and Clients yields the HIC vacancies, while the ratio of Clients to HIC Beds yields the HIC Bed Utilization Rate.

It is important that providers review HIC bed capacity data to ensure that this is still representative of the project since project capacity can fluctuate throughout the year. Census reporting also underscores the importance of timely enrollment and discharge data. HIC project inventory may need to be expanded or contracted annually to accommodate changes in capacity. The HMIS Lead is aware that new projects may need additional time to ramp-up and reach capacity. Utilization rates higher than 100 percent or lower than 70 percent may indicate data entry issues or problems filling vacancies. Funders or program managers may want to use these reports to improve operations or identify areas for improvement.

III. HMIS Security and Privacy Plan

A. Introduction and Background

This HMIS Security and Privacy Plan (SPP) sets standards for the privacy and security of personal client information collected and stored in the HMIS. The SPP seeks to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. The standards set forth in this SPP are based on principles recognized by information privacy and technology communities.

The SPP provides a framework that mirrors many of the technical standards laid out in the 2004 HUD HMIS Data and Technical Standards, while supplementing that documentation with specific policies that have been developed and implemented throughout BTG, and action steps that all organizations utilizing the HMIS are expected to apply. The SPP outlines baseline standards that will be required by any organization that records, uses, or processes protected personal information (PPI) on homeless clients for an HMIS. The SPP strives to reference procedures that organizations and stakeholders can utilize to enhance the privacy and security of information collected through the HMIS.

Throughout the SPP, baseline standards for evaluating privacy and security requirements will be established. At a minimum, all organizations that record, use, or process PPI on homeless clients must meet these baseline privacy and security requirements. This approach provides a standard level of protection for homeless clients and allows for the possibility of additional protections for organizations with additional needs and resources.

B. Key Terms and Definitions

CoC Program: A program identified by the CoC as part of its services system, whose primary purpose is to meet the specific needs of people who are experiencing a housing crisis.

Continuum of Care (CoC): The primary decision-making entity defined in the funding applications to HUD as the official body representing a community plan to organize and deliver housing and services to meet the specific needs of people who are homeless as they move to stable housing and maximum self-sufficiency

Contributory HMIS Organization (CHO): An organization that operates a contributory homeless assistance program or homelessness prevention program or contributory non-homeless assistance program.

End User: An employee, volunteer, affiliate, associate, and any other individual acting on behalf of a CHO or HMIS Lead Agency who uses or enters data into the HMIS or another administrative database from which data are periodically uploaded to the HMIS.

Homeless Management Information System (HMIS): The information system designated by a CoC to process Protected Personal Information (PPI) and other data to create an unduplicated

accounting of homelessness within the CoC. An HMIS may provide other functions beyond unduplicated reporting.

HMIS Administrator: A local administrator established by the HMIS Lead to act as the point of contact for many HMIS related questions. The HMIS administrator works with stakeholders and CHOs as a conduit for localized HMIS technical assistance.

HMIS Lead: The organization designated by BTG to operate the HMIS on its behalf.

Homeless Programs Office (HPO): State office housed under the Hawaii Department of Human Services, responsible for the administration of many homeless assistance programs statewide.

Protected Personal Information (PPI): Information about a client: (1) whose identity is apparent from the information or can reasonably be ascertained from the information; or (2) whose identity can, considering any methods likely to be used, be learned by linking the information with other available information or by otherwise manipulating the information.

C. HMIS Privacy Standards

The goal of the HMIS Privacy Standard is to ensure that all required client data will be entered in the Hawaii HMIS while maintaining the confidentiality and security of the data in conformity with all current regulations related to the client's rights for privacy and data confidentiality.

1. HMIS Privacy Policy Notice

Policy: All CHO that enter data into the HMIS must have an HMIS Privacy Notice posted at their workstation or wherever data is collected and entered, which describes how information about the client may be used and disclosed and how the client can get access to their information. The HMIS Privacy Notice is a brief document describing a consumer's data rights in relation to the HMIS. Agencies MUST use the sample documents attached in Appendices 1 and 2.

Procedures: Each workstation, desk, or area used for HMIS data collection must post the HMIS Privacy Notice. As Outreach workers gather data in the field, they should have the Privacy Notice visible to all clients. This policy will allow Outreach agencies to use an implied consent model, as outlined within this section. If an agency serves non-English-speaking clients, or clients whose primary language is not English the agency must also provide translation services for the HMIS Privacy Notice. If an agency has a website, the HMIS Privacy Notice must be posted on that website as well. An agency may also post the HMIS Privacy Notice in a waiting room, an intake line, or any other public area where clients congregate before intake occurs.

2. HMIS Client Consent Form (Release of Information)

Policy: All clients must sign the HMIS client consent form before their PPI can be shared with other agencies in the HMIS. Client information can be entered into the HMIS without consent; however, this information cannot be shared with other organizations. All HMIS client consent forms must be stored securely for a minimum of seven years after the client last received services from the agency and uploaded in HMIS. Agencies must give a copy of the consent form to clients if requested. BTG's HMIS client consent form is available on the BTG website.

Procedures: Each adult client reads and signs the HMIS client consent form before their information and information for their dependents may be shared with other agencies in the HMIS. The HMIS client consent form is valid for three years from the date of signature whereby the client consents to share their data. It is important to keep the consent form collected for auditing purposes for at least seven years. Consent forms must be kept securely in accordance with standard confidentiality and privacy practices (e.g., locked in a file cabinet and not accessible without authorization).

It is recommended that agencies keep the consent form with the established client file along with other information that is being collected and maintained. Agencies may also wish to voluntarily give all clients copies of their signed client consent form.

3. Offsite Data Entry

Policy: Outreach providers and other HMIS users can collect client level data in many different settings including the street, places not meant for human habitation, or on site. Because these locations are not ideal for data entry, outreach providers must not enter client-level data into the Hawaii HMIS through tablets or other wireless devices via an unsecured wireless network.

Procedures: Outreach providers and other HMIS users must ensure that internet connections used to access the HMIS from their facilities are set up using basic standard network security protocols to prevent unauthorized access to the network and to HMIS data stored in local servers or hard drives.

Because of the confidential nature of data stored within HMIS, the system must be accessed from a sufficiently private physical location to ensure that persons who are not authorized users of the HMIS are not able to view client level data.

Because these standards are important for the protection of client-level data, outreach providers and other HMIS users must not enter client level data over unsecured public wireless internet connections to safeguard transmission of client PPI. Outreach providers and other HMIS users should gather information on paper for data entry when a secure internet connection can be established.

4. Presumed Client Competence

Policy: Unless a court order claiming incompetence is known or provided, clients are presumed competent when filling out the HMIS client consent form. Organizations should presume that all clients are competent unless there is a known court ordering stating otherwise or obvious assessment to the contrary can be made.

Procedures: If there is a known court order stating the individual is not competent, then it will not be possible to obtain client consent for the HMIS. In this case, CHO end users may enter client information into the HMIS, however, that information must not be shared with other CHOs.

CHO end users should do their best in attempting to obtain consent to share from individuals that may not appear to be fully competent during intake when there is no court order.

5. Denial of Services

Policy: Clients do not have to participate in the HMIS or sign the client consent form to receive program services. Agencies cannot deny services to an individual solely based on the individual deciding not to participate in HMIS. Some clients will choose not to share data in the HMIS or will not be capable of making an informed consent; however, it is important that these clients are not prohibited from receiving services by the program.

Procedures: If a client decides not to share their data in the HMIS, an agency cannot deny services because of that decision. Agencies are not required to guarantee services to an individual, however, as they may fail other eligibility criteria, lack of openings, and/or lack of funding. Agencies may determine if an individual will or will not receive services before the individual goes through the informed consent process. This will eliminate a perceived relationship between HMIS participation and service delivery. Clients that elect not to share their data within HMIS will limit the ability of the Coordinated Entry System to quickly house the client.

6. Workstation Privacy

Policy: In an effort to keep the HMIS and client data secure, end users and CHOs must implement the following security measures.

A. End user's computer screens should be placed in a manner where it is difficult for others in the room to see the contents of the screen. Workstations should not be in common areas where clients or other non-HMIS staff can gain access.
B. End users should not write down usernames and passwords and store them in an unsecured manner. This includes posting password and/or login information visibly near the workstation.
C. When end users are away from the computer, they should log out of the HMIS or lock down their workstation.
D. Computers used for HMIS data entry or analysis must have locking screensavers with password protection. Screensavers should lock after five minutes of inactivity

Procedures: The following procedures correspond with the above policy requirements and are mandatory for all CHOs.

A. Monitor placement plays a role in establishing security within an organization. End users should consider placing the monitor in a manner so that it is difficult for others to see the screen. This will help to protect the privacy of client PPI.
B. Never post HMIS login and password information under your keyboard, on your monitor, or out in the open. Implementation of this policy will make it much more difficult for others to obtain your login information and achieve access into the HMIS.
C. End users stepping away from their computers must log completely out of the HMIS. Locking down the workstation is also a good policy if PPI is stored locally.
D. CHO IT departments must implement locking screen savers on all computers used for HMIS data entry or analysis.

7. Password Privacy Requirements

Policy: It is imperative that end users never share their login information with anyone; including coworkers or managers. Each end user must fill out an HMIS user agreement form and have distinct login information that is not shared. Additionally, when HMIS end users leave or are terminated from the organization, the Agency Administrator must deactivate the user and notify the HMIS administration team through the ticket system within 24 hours so that the end user can be removed from the HMIS.

Procedures: If someone is having trouble accessing the HMIS or has been locked out of the system, please advise them to contact the HMIS administration team through the ticket system. Sharing login information with another person is a direct violation of the HMIS user agreement and this Plan. End users and their CHO are ultimately responsible for all actions occurring in the system under their login information. Auditing and access log functionalities are part of the HMIS, which implies that specific user tasks and procedures can be traced.

All CHO end users must fill out and email a completed HMIS user agreement to the HMIS Administration team before access will be established via the ticket system. A copy of the current Hawaii HMIS user agreement is on the BTG website. **The HMIS Administration Team must be apprised within 24 hours when HMIS end users exit employment voluntarily, are terminated, or are laid off**. These users will need to be deactivated from the HMIS. CHOs repeatedly failing to adhere to this policy may see funding adversely affected.

8. HMIS Data Sharing

Policy: HMIS client data cannot be shared with other organizations unless explicitly authorized by the client through the client consent form. Currently, all organizations have the potential to share data except RHY providers that can only share data in certain circumstances (RHY programs whose participants are over 18 years of age with a signed consent or under 18 years of age with a signed consent by parent or guardian). HIV/AIDS,

mental health, and substance use providers can share data with appropriate informed consent. Data sharing must be manually selected for each client for it to take effect.

Procedures: The HMIS is capable of sharing client historical data, which includes services and basic demographic data including, but is not limited to: name, age, gender, race, ethnicity, family members, marital status, any history of domestic violence, housing history, disabling conditions, VI-SPDAT survey data, program intake dates, encounter dates, program discharge dates, employment status, income and non-cash benefits, health insurance, case notes, eligibility documents, and housing plan. It should be noted that a client's SSN and DOB are part of the search.

CHO users will always keep client data confidential and will obtain client consent to share client PPI via the HMIS. The HMIS application allows agencies to share service records, which allows them to coordinate services more efficiently. Part of the CoC monitoring policy will be to ensure that client's electing to share data on paper were also selected to share data via the HMIS. This policy aligns with the sections above.

9. Client Access to Their Records

Policy: Clients have the right to receive a copy of their data that is entered into the HMIS. This policy must be present in the HMIS Privacy Notice and is outlined in the above section. Agencies must be able to accommodate this item but are advised not to make copies for clients unless it is requested. Client's may lose or misplace PPI via paper forms, which may increase the likelihood of the information being used for malicious purposes.

Procedures: Clients may request a copy of their information contained within the HMIS. Agencies are required to provide them with a copy of the universal and program specific information if it is requested. Agencies are not required to print out any additional information, although it is optional and allowed.

10. Client Grievance Process

Policy: Clients have the right to file a grievance with the CHO concerning violations of their privacy rights regarding their HMIS participation. No action or punishment may be taken against a client if they choose to file a grievance.

Procedures: A client must request and complete the CoC's standard grievance form. The client may turn the form into an organization not related to the grievance or may mail the form to the CoC.

The CoC will review the grievance, research the nature of the complaint, and will respond to the grievant within 30 days. The agency named in the grievance, the CoC, and other participating HMIS agencies will not refuse or reduce services to the client because of a filed grievance. A thorough investigation by CoC will ensue if a client reports retaliation due to the filed grievance.

11. Research Agreements

Policy: Research agreements between various organizations may be enacted for the purposes of analysis and dissemination of HMIS data. This research may be conducted so long as agreements are drafted between organizations before data is supplied or received. Conclusions and analysis must be presented in the aggregate and must not display any client PPI. The BTG Data Committee and HMIS Lead will review data requests.

Procedures: Formal, written agreements must be established between organizations before HMIS data is supplied.

12. Data Integration Requests

Policy: Agencies who use CaseWorthy as their internal client management system may request to integrate their data into HMIS.

Procedures: All data integration requests are to be sent to the BTG Data Committee Chair for consideration. The request must detail the following:

- The Name of the Organization and Associated programs
- Rationale for data integration
- Mission of Organization and Associated programs
- Continuum(s) of Care where services are provided
- Services provided by the Organization and Associated programs
- Describe how data integration will better serve clients and more efficiently and effectively end homelessness
- Describe how costs of the data integration will be managed
- Describe the frequency of data integration and the data integration flow (one-way or two-way, real time or batched)
- Describe how the data quality and data improvement process will work without involvement of the HMIS Lead or HMIS System Administration
- Describe how the organization will coordinate and communicate during the data integration testing, implementation, and ongoing management phases
- Describe why the organization operates an internal comparable database and does not adopt the HMIS as the internal database (be specific about required use of the database by funders)

The BTG Data Committee will make a recommendation on the data integration request with a simple majority vote of a quorum of the voting members. If the Committee recommends data integration, the data integration request will be sent to the BTG BOD for formal approval. If the Data Committee does not recommend data integration, the Organization will be notified via e-mail by the Data Committee Chair and will be offered a rationale for the decision to deny the data integration request.

IV. HMIS Security Standards

The goal of the HMIS Security Standards is to ensure that HMIS data are collected, used, and always maintained in a confidential and secure environment. The HMIS Security Standards applies to the HMIS Lead, CHOs, and the overall HMIS software solution. Specific applicability is described in each policy within these security standards. These standards apply to all PPI collected in the HMIS or uploaded through comparable databases.

The HMIS Lead recognizes that agencies may have established their own security policies that meet the HUD security requirements and minimum standards set forth below. The chief purpose of this document is to outline those standards to all CHOs and define the parameters of compliance with these standards. This document is not intended to supplant individual CHO security policies, but rather to supplement them. If CHO policies and practices meet the minimum thresholds established in this plan, they may establish additional or more stringent security requirements. Another key purpose of this document is to describe how the HMIS Lead will meet and maintain security requirements established in HUD's security standards.

A. Levels of User Access and Security

Policy: Each CHO will maintain a written policy detailing organizational management control over access authorization, user levels, and the internal process for activating new HMIS users. BTG will be solely responsible for authorizing new agency access to the HMIS and the HMIS Administration Team will be solely responsible for establishing new users in the HMIS. The highest HMIS access level of system administrator will only be assigned to the HMIS Lead and the associated HMIS Administration Team.

Procedures: CHOs must establish an internal point of contact that will be the conduit for establishing new users with the HMIS administration team. Individual staff should not email or request new HMIS users with HMIS Lead or the HMIS Administration team. This is important from a security standpoint, as staff may no longer be employed with the organization.

The Hawaii HMIS has the following user types:

Agency level discretion:

- **Case Management** – For entering client demographics and enrolling clients into programs or exiting them from programs.
- **Agency Admin** – For running program and agency level reports specific to an organization. All reports are based on information entered via HUD assessments.
- **BTG VI-SPDAT** - For entering VI SPDAT assessments, checking Coordinated Entry System (CES) readiness and receiving/processing CES referrals.

System level discretion:

- **BTG Coordinated Entry** – For Coordinated Entry System (CES) Administrators who run By-Name Lists (BNL) and make CES referrals in their respective counties.

- **Hawaii All Features** – For HMIS system level administrators to carry out system level responsibilities like program set up, reports development and database feature modifications.

The CHO point of contact(s) must also maintain listings of active users and notify the HMIS Administration team immediately if any HMIS users are no longer employed with the agency.

B. Security Incident Procedures

Policy: Security incident procedures elicit a two-tiered approach:

1) A user who breaches the terms of the HMIS user agreement will face sanctions specified by the CoC so that repercussions are uniform and fair for all CHOs. These specifications are required to be documented as part of the HMIS security plan. Any breaches related to security or privacy must be reported to the HMIS Lead within three business days of discovery. These breaches will be dealt with on a case-by-case basis by the HMIS Lead. The CHO assumes all responsibility for negligence due to data breaches or risk of incident within the organization.

2) All HMIS users are obligated to report suspected instances of noncompliance with these Standards that may leave HMIS vulnerable to intrusion or compromise client PPI. The HMIS Lead and HMIS Administration team are responsible for reporting any security incidents involving the real or potential intrusion of the HMIS to the CoC. Each CHO is responsible for reporting any security incidents involving the real or potential intrusion of the HMIS to the HMIS Lead Agency.

Procedures: Associated measures for dealing with suspected or actual breaches of the HMIS in accordance with the above policies are outlined below.

1) Penalties may include but are not limited to a temporary or permanent ban from using the HMIS and legal action. The CoC has implemented baseline written policies for managing a breach of the HMIS user agreement. The CHO Agency Administrator should use all reasonable measures to ensure staff complies with these policies. At minimum, CHOs will inform users that unauthorized use or disclosure of PPI is considered a serious matter and will result in penalties or sanctions, which may include:

a) The loss of use or limitation on the use of the HMIS and other office and technology resources
b) Financial liability for any costs that may arise through user negligence
c) Adverse employment actions including dismissal
d) Civil and/or criminal prosecution and penalties

Each CHO will indicate in the Security Certification Checklist (Appendix) whether such a policy exists. If such a policy does not exist one year from the date of execution of this Plan, the CHO must establish a date not later than three months from the annual date by which

such a policy will be developed and implemented. A copy of the policy must be provided to the CoC by the target date.

2) HMIS users will report any incident in which unauthorized use or disclosure of PPI has occurred. CHO users will report any incident in which PPI may have been used in a manner inconsistent with the HMIS Privacy or Security Standards. Security breaches that have the possibility to impact the Hawaii HMIS must be reported to the Agency Administrator, HMIS Administration team, the CoC, and HMIS Lead. Each CHO will maintain and follow CoC-wide procedures related to thresholds for security incident reporting.

The CoC and HMIS Lead Agency staff, in conjunction with the HMIS Administration team and CoC, will review violations and recommend corrective and disciplinary actions. Each CHO will maintain and follow procedures related to internal reporting of security incidents.

C. Audit and Access Controls

Policy: The Hawaii HMIS will maintain an accessible audit trail that allows the monitoring of user activity.

Procedures: The use of the HMIS audit trail will be used in situations of misusage of HMIS by the HMIS System Administration Team, HMIS Lead and CoC to the penalties listed in "Security Incident Procedures".

D. Personnel Authentication & Password Protocols

Policy: To the extent possible, a background check should be initiated for all users prior to the provision of HMIS access. If a background check is completed, any user with history of crimes related to identity theft or fraud must not be allowed access to the HMIS.

The below outlines password and user inactivity protocols for the Hawaii HMIS:

1) All passwords must be unique,
2) All passwords must be rotated every three months,
3) All passwords must be in a prescribed format,
4) Upon the third unsuccessful login try, users will be locked out of the system and prompted to reset their password with the HMIS "forgot my password" feature. If that fails, users should contact the HMIS administration team to reset.
5) All users with no login activity for at least three months will be automatically deactivated.

Procedures: Organizational policy should mandate the denial of access to personnel that have criminal history relating to identity theft or fraud. Relating to items one through five above, all passwords must be unique and in the prescribed format as indicated on the initial HMIS login screen. Passwords for active users must be rotated every three months via HMIS prompt. After three unsuccessful login attempts, the HMIS will automatically lock out the user and the user will be prompted to reset their password with the HMIS "forgot my password" feature. If that fails, users should contact the HMIS administration team to reset.

All users with no login activity for at least three months will be automatically deactivated. The HMIS Administration team must be notified and will then have to reactivate.

E. Malware and Virus Protection with Auto Update

Policy: All CHOs accessing the HMIS must protect the system by using commercially available malware and virus protection software. CHOs must also protect the workstations accessing the HMIS system from malicious intrusion by maintaining a secure firewall.

Procedures: Virus and malware protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is accessed. A CHO must regularly update virus definitions from the software vendor. There must be a firewall between the workstation and any systems, including the Internet and other computer networks, located outside of the organization.

F. Disaster Protection and Recovery

Policy: The HMIS vendor must have a plan for maintaining and recovering access to HMIS data in the event of disaster.

Procedures: The HMIS vendor will include provisions to maintain a backup of the HMIS data at a separate physical location consistent with the most up-to-date HUD HMIS security standards. The HMIS hosting entity will back up all HMIS data daily. All backups will be held securely at a secondary data center within the hosting entity. To the extent possible, all data will be copied to a second server so that if an entire server malfunctions, data will be available immediately with no service interruption. The failover function will be tested at least once per year and after each major system upgrade.

G. Hardware/Software Management & Physical Safeguards

Policy: The HMIS vendor will ensure that the hosting entity maintains protections for the physical security of the facilities and media in which HMIS data is stored.

Procedures: Physical safeguards within the hosting entity include secure site storage, power grids, uninterrupted power supplies, air conditioning, and disaster prevention and recovery systems. The HMIS vendor will utilize multiple hard drives and redundant power supplies to minimize interruption to service. At a minimum, the HMIS data will be stored in a facility with appropriate temperature control and fire suppression systems. Surge suppressors must be used to protect systems used for collecting and storing all HMIS data.

H. Wireless Transmission Security

Policy: The HMIS vendor is responsible for ensuring that HMIS SSL certificates are kept current. CHOs will specify in their security standards that sensitive PPI such as SSNs will not be transmitted over the internet through email accounts. Policies regarding the transmittal of HMIS username and password information must be established and assert that

each piece of login information must not be sent in the same email. Users accessing the HMIS outside of the workplace are held to all standards within this Plan and assume all risk associated with potential breach of HMIS data.

Procedures: SSL (Secure Sockets Layer) is standard security technology for establishing an encrypted link between a website and a browser. SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. The SSL protocol determines variables of the encryption for both the link and the data being transmitted. It is the responsibility of the HMIS vendor to retain a current certificate.

Each CHO must establish policies within its security plan so that PPI is not transmitted over the internet via email. Username, password, and HMIS URL information must not be sent in the same email as a defense against potential threats to the HMIS. Users accessing the HMIS outside of the natural work environment are expected to adhere to the same policies as outlined in this Plan. Wherever possible, information should be sent over the phone to communicate usernames and passwords with HMIS end users.

I. CHO Data Safeguards Outside of HMIS

Policy: Any CHO that downloads client-level data from the HMIS will take full responsibility for safeguarding the data with the same security and privacy protocols as outlined in the HMIS Policies and Procedures. This policy is for HMIS client records as well as any reports where client level information is included such as a By Name List.

Procedure: Any CHO or HMIS user assigned to a CHO will be held responsible should client-level data be removed from HMIS and not protected to the standards set forth in the HMIS Policies and Procedures. The most likely source and risk for a client-level data breach is data downloaded from the HMIS and managed improperly at the CHO-level. Each agency will have an annual review (Security Certification Checklist Appendix) by the CHO designated Agency Administrator that affirms any data removed from HMIS is protected to the standards laid out in the HMIS Policies and Procedures. Failure to follow this process could lead to the CHO losing access to HMIS.

V. HMIS Policy and Procedures Appendices

Appendix 1: Privacy Policy

PRIVACY POLICY

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN OBTAIN ACCESS TO THAT INFORMATION. PLEASE READ IT CARFULLY

Effective Date:_____

Our Duty to Safeguard your Personally Protected Information (PPI):

_____(Agency Name) collects information about the clients that utilize services that we provide. We will ask for your permission to share the information we collect about you and your family (as applicable) in a program called the Homeless Management Information System (HMIS). Although the HMIS helps us keep track of your information, individually identifiable information about you is considered PPI. We are required to protect the privacy of your identifying information and to give you notice about how, when, and why we may use or disclose the information.

We are required to follow the privacy practices described in this Notice. The Bridging the Gap (BTG) is responsible for updating this Privacy Policy annually and can make changes at any time.

_____(Agency Name) may have additional internal privacy protocols and may change their privacy protocols at any time. As a client you have the right to request the most up to date agency privacy policy.

How We May Use and Disclose Your Information:

We use and disclose collective information for a variety of reports. We have a limited right to include some of your information for reports on homelessness and services needed by those who are homeless. Information that could be used to identify you will never be used for these reports. If you are enrolled in the Supportive Services for Veteran Families (SSVF) Program, your information will be shared as mandated by the Department of Veteran Affairs.

We may use your information in approved research requests. We must have your written consent to use or disclose your information unless the law permits or requires us to make the use or disclosure without your permission. Please review the client consent form for further details.

Your Rights Regarding Your Information:

- You have the right to receive services even if you choose NOT to participate in the Hawaii HMIS. However, clients may be refused program entry for not meeting other agency eligibility criteria.
- You have the right to ask for information about who has seen your information.
- You have the right to view your information and change it if it is not correct.

Appendix 2: Privacy Notice (Posted Sign)

Bridging The Gap Continuum of Care (BTG)

Homeless Management Information System (HMIS)
Mandatory Data Collection Notice

We collect personal information directly from you for reasons that are discussed in the HMIS privacy policy. We may be required to collect some personal information as mandated by law or as requested from organizations that fund this program. Other personal information we collect is necessary to operate programs, improve services, and better understand the needs of homelessness. We collect appropriate information only. The HMIS Privacy Policy is available upon request.

Appendix 3: Privacy & Security Certification Checklist

All Contributing HMIS Organizations must comply with the following privacy and security certifications annually. All organizations will be monitored according to the following checklist at least once every two years.

Section	Policy Requirement	Meets Requirement (Y/N)	If No, date when will be met
III.C.1	Posted HMIS privacy Notice at all CHO workstations or where data collection occurs and the HMIS Privacy Policy is available upon request.		
III.C.2	CHOs have the most current HMIS client consent form. Sampled clients entered in the HMIS have a valid consent form. The consent and intake information are kept in a secure location.		
III.C.6	Screens where HMIS data entry occurs are placed in a manner making it difficult to oversee information being entered.		
	User login information are not left out in the open.		
	Locking screensavers (5 Min) are functional at workstations		
III.C.7	CHO follows the HMIS security policy for deactivating personnel within 24 hours of the end of their employment and communicate this change with the HMIS Lead.		
III.C.8	CHO follow the HMIS policy for sharing data via the HMIS. Clients sampled for which data sharing is checked in the HMIS contain appropriate consent forms.		
III.C.9	CHO follows the HMIS privacy policy that contains wording expressing client's right to receive a copy of their information entered in the HMIS.		
III.C.10	CHO follows the HMIS security plan for grievances associated with violations of privacy rights regarding HMIS participation. A formal CoC grievance process has been established and utilized.		
IV.A	CHO follows the HMIS security plan and details organizational control and accounting of active HMIS users. POCs have been established to communicate with the HMIS Lead.		
IV.B	CHO follows the HMIS security plan that addresses measures for dealing with suspected or actual HMIS security breaches.		
IV.D	Public workstations with access to the HMIS must have security measures such as locking screensavers or program staff monitoring.		
IV.E	CHO workstations must have malware and virus protections with auto updates.		
IV.G	Physical safeguards for protection of HMIS data must be in place at the organizational and administrative levels.		
IV.H	CHO must follow the HMIS security and privacy policies regarding the transmittal of PPI and user login and password information via email.		