CLARITY
HUMAN SERVICES

Clarity Nevada HMIS Governance

State of Nevada CoCs

HMIS Governance Charter v4.0

(702) 614.6690
(800) 594.9854

www.bitfocus.com

Bitfocus

TABLE OF CONTENTS

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXECUTIVE SUMMARY

HMIS Overview

The United States Department of Housing and Urban Development (HUD) defines the Homeless Management Information System (HMIS) as the information system designated by the Continuum of Care (CoC) to comply with HUD's data collection, management, and reporting standards. The HMIS collects data to measure the efficacy of services provided to homeless persons and those persons at risk of homelessness. It is intended to generate unduplicated counts of homeless persons, as well as explore the nature of homelessness in general. The data collected by the HMIS are used to drive evidence-based decisions at the local, state, and national level, with the ultimate goal to eradicate homelessness in the United States.

This document outlines the state of Nevada HMIS Governance structure, and provides the policies, procedures, guidelines, and standards that govern state of Nevada HMIS operations, while dictating the roles and responsibilities of all parties involved.

State of Nevada HMIS Governance Charter

This state of Nevada HMIS Governance aims to provide structure for decision-making, as well as formalize the roles and responsibilities of all HMIS entities. It defines the relationship between the HMIS implementation, the three Nevada Continuums of Care, and the participating providers, and establishes oversight and leadership expectations surrounding the HMIS.[1]

[1] There exists three Continuums of Care within the State of Nevada. Although these Continuums of Care operate independently of one another, they collaborate on all matters pertaining to the HMIS.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Nevada HMIS Governance Model

The state of Nevada HMIS governance model is that of a HMIS Working Group. This HMIS Working Group is comprised of the following:

- CoC Representatives
- HMIS Lead Agency Staff (Clark County Social Service)
- Local Jurisdictional Representatives
- Participating Agency Staff and Consumers

However, in this governance model, the three Nevada Continuums of Care are collectively responsible for all final decisions regarding the planning of policies and procedures, coordination of resources, data integration, determination of software applications, while also directing the HMIS lead agency.

The role of the statewide HMIS Working Group is further defined in a MOU among all three Nevada CoC and the HMIS Working Group Governance. It should be noted that not all items need to go before the statewide HMIS Working Group, only those items that affect the entire system. Further, each NV CoC has their own local HMIS Working Group that is designated by the CoC to oversee HMIS.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

DESIGNATIONS

The main entities included in this HMIS Governance Charter are as follows:

Nevada Continuums of Care (CoC)

The entity is composed of 3 Nevada Continuums of Care; Southern Nevada, Northern Nevada, and Rural Nevada/Balance of State. Each consists of representatives of relevant organizations in the state of Nevada, which generally includes nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve homeless and formerly homeless veterans, and homeless and formerly homeless persons that are organized to plan for and provide, as necessary, a system of outreach, engagement, and assessment; emergency shelter; rapid re-housing; transitional housing; permanent housing; and prevention strategies to address the various needs of homeless persons and those persons at risk of homelessness for the state of Nevada.

HMIS Administrator (Bitfocus Inc.)

The entity designated by the state of Nevada CoC to oversee the day-to-day administration of the HMIS system, overseen by the HMIS Lead Agency (Clark County).

HMIS Lead (LV/CC CoC Coordinator)

The duties of the HMIS Lead are:

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

- Ensure all recipients of funds from the Emergency Solutions Grants Program (ESG) and programs authorized by Title IV of the McKinney-Vento Act participate in HMIS
- Develop written policies and procedures for all Covered Homeless Organizations (CHOs)
- Execute an HMIS participation agreement with each CHO
- Serve as the applicant to HUD for any HMIS grants that will cover the CoC geographic area
- Monitor compliance by all CHOs with the CoC
- Submit a Security Plan, Data Plan, Data Quality Plan, and a Privacy Plan to the CoC for approval within 6 months of the finalization stage of the HMIS Requirements Proposed Rule. These documents must be reviewed and updated annually. Implementation of the policies outlined in the plans must be implemented within 6 months of the date of CoC approval of the plans

Note: The HMIS Lead will execute system-wide decisions regarding the HMIS made by the HMIS Working Group. These decisions will impact all CHOs within all three CoC.

HMIS Working Group

Group of entities that provide recommendations on use of software, software enhancement, and system-wide HMIS policy.

At least one homeless person or formerly homeless person must participate in policymaking. Participation can include but is not limited to the following entities (as defined by HUD): governing board leadership, advisory committees, staff positions, and sub-committee positions. The statewide HMIS Working Group is further defined in a MOU between all three Nevada CoC and the statewide HMIS Working Group Governance.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

HMIS Software Application

The CoC has designated Clarity Human Services software to serve as its HMIS. Clarity Human Services software is a product of Bitfocus, Inc., and will hereafter be referred to as the Clarity System.

Participating Agencies

Any agency that makes reasonable efforts to record all HUD-defined Universal Data Elements and all other required data elements as outlined by HUD funding requirements on all clients served, and discloses these data elements to the HMIS Lead Agency.

Any agency providing homeless services and wishing to participate in HMIS will complete and submit a HMIS Participation Agreement application. This application is reviewed by the HMIS Lead for approval. In the event there is a question regarding the need to participate, the application is taken to the HMIS Working Group for approval/denial.

The HMIS Working Group has given the HMIS Lead authorization to approve applicants to use HMIS if the HMIS Lead is confident that the applying agency is serving the homeless population.

HMIS Funding

HMIS Leads and CHOs must refer to program regulations to determine how funds are made available. Program regulations for the HUD McKinney-Vento Act programs can be found in the regulations of Chapter V of title 24 of the Code of Federal Regulations. These regulations explain how funds are made available, and the requirements attached to those funds.

ESG & McKinney-Vento Act funding recipients and sub-recipients must participate in the Clarity Nevada system. Only homeless service providers receiving CoC and ESG funding can access HMIS funding.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

STATUTORY AUTHORITY

The implementation of the McKinney-Vento Act in1987 created valuable programs aimed to assist homeless persons or persons at risk for homelessness regain independence and stability.[1] However, despite its promising beginnings, the McKinney-Vento Act, and the programs it fostered, operated without measurement of efficacy for over 15 years; no government entity conducted a comprehensive review. Therefore, in 2001, Congress enlisted the U.S. Department of Housing and Urban Development (HUD) to enforce the requirement that every jurisdiction present to Congress unduplicated client-level data within three years.[2]

HUD formulated a strategic plan to test the efficacy of the McKinney-Vento Act while also improving data collection, reporting, and analysis at the local and national levels. [2] Their strategy consisted of four approaches:[5]

1. They established funding for the implementation and maintenance of HMIS.
2. They created a technical assistance program to assist jurisdictions in their data collection, analysis, and reporting efforts.
3. They initiated the development of the nationwide Annual Homeless Assessment Report (AHAR) as means to present to Congress collective homeless data from individual jurisdictions nationwide.
4. They began to analyze the most viable approaches to obtaining homeless client-level reporting

This plan amplified competition among CoCs as they strived to obtain homeless assistance funding. As the importance of HMIS applications increased, so did their complexity and sophistication.

CoCs became increasingly aware of the data collection and reporting requirements imposed by Congress, and in 2004, HUD submitted their Third Progress Report to Congress. [3] As a result, Congress and HUD implemented the first HMIS Data and

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Technical Standards Final Notice. This Notice made the implementation and maintenance of HMIS mandatory to obtain Federal funding for homeless relief efforts.[4] In following years, the HMIS requirements were further modified.[5] Currently, CoC's are awaiting the implementation of the upcoming HMIS Requirements Proposed Rule.[6]

Collectively, these provisions provide statutory requirements for this governance charter, which aims to organize the accurate collection and reporting of comprehensive data regarding the characteristics and needs of homeless persons and those at risk of homelessness.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

POLICIES & PROCEDURES

The following policies and procedures are primarily derived from the 2004 HMIS Data and Technical Standards: Final Notice [4] and the most current HMIS Data Standards[5].

Note that this governance charter will be updated upon the finalization of the HMIS proposed rule.[6]

This section is comprised of six (6) sections:

1. Planning & Software Selection
2. HMIS Management & Operations: Governance & Management
3. HMIS Management & Operations: Compliance Monitoring
4. HMIS Management & Operations: Data Quality
5. HMIS Development & Oversight
6. Other Federal Requirements

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

1. Planning & Software Selection

The following policies and procedures are derived from the most recent HUD HMIS Requirements.

1.1 HMIS Planning & Strategic Activities

Development of activities related to HMIS growth. These activities will be reviewed regularly, and remain in accordance with the CoC's goals.

Responsible Party
HMIS Lead with direction from the HMIS Working Group

1.2 HMIS Program Milestones Development

Identification of general milestones for project management, including training, expanded system functionality, etc.

Responsible Party
HMIS Working Group and 3 Nevada CoC

1.3 Universal Data Elements

HMIS must be equipped to manage the collection of each data variable and corresponding response categories for the Universal Date Elements as outlined in the most current HMIS Data and Technical Standards.[5]

Although HUD strives to ensure that the HMIS remains "*a system of accuracy, integrity, and confidentiality*" they are aware that excessively stringent technical, security, and

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

data standards may limit the ability of CoCs to adapt to beneficial changes in technology. Therefore, the standards listed in the following section are broad in nature. HUD states they will provide specific details applicable to each area in a separate notice and public comment process, thus enabling them to be more responsive to changes in technology.

Proposed Requirements:

- HMIS must be capable of unduplicating client records, must contain fields that collect all HUD-required data elements, and must maintain historical data
- HMIS must generate Standard HUD Reports, Data Quality Reports, and Audit Reports

Responsible Party
HMIS Lead

1.4 Program-Specific Data Elements

HMIS manages the collection of each data variable and corresponding response categories for the Program-Specific Data Elements as outlined in the most current HMIS Data and Technical Standards.[5]

Responsible Party
HMIS Lead

1.5 Unduplicated Client Records

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

HMIS generates a summary report of the number of unduplicated client records that have been entered into the HMIS.

Responsible Party
HMIS Lead

1.6 APR Reporting

HMIS is consistently able to produce a reliable Annual Performance Report (APR).

Responsible Party
HMIS Lead

1.7 AHAR Participation

Participation in the AHAR (Annual Homeless Assessment Report) is ensured.

Responsible Party
3 Nevada CoC with Guidance from HMIS Administrator

1.8 HMIS Reports

HMIS generates clients-served reports, utilization summary reports, and demographic reports at both the system and program levels for the purpose of understanding the nature and extent of homelessness.

Responsible Party
HMIS Lead

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

2. HMIS Management & Operations: Governance & Management

2.1 HMIS Governance Structure

Development of a HMIS governance model that is formally documented between the HMIS Lead Agency/grantee and the community planning body(ies). This document is to be a formal agreement that outlines management processes, responsibilities, decision-making structures, and oversight of the HMIS. Adherence to the agreement is to be regularly monitored (as evidence by a Memorandum of Understanding, Letter of Agreement, or similar such documentation).

HMIS Governance Standards;

- HMIS Lead is responsible for implementation of local HMIS policies and procedures developed by the HMIS Working Group.
- HMIS Lead and CHO are responsible for ensuring that HMIS processing capabilities coincide with the privacy obligations of the CHO.
- HMIS Lead must conduct annually (at minimum) an unduplicated count of clients served and an analysis of unduplicated amounts. This information is to be presented to the CoC and when requested by HUD.
- HMIS Lead must submit reports to HUD as required.
- CHO must comply with applicable standards from HMIS Requirements Proposed Rule.
- CHO must comply with federal, state, and local privacy laws. If a privacy or security standard conflicts with other federal, state, and local laws, the CHO and HMIS Lead are jointly responsible for updating the policies and procedures.
- HMIS Lead must develop a privacy policy with guidance from the HMIS Working Group.
- HMIS Lead must ensure HMIS vendor acts in accordance with HMIS standards issued by HUD.

Responsible Party
HMIS Working Group and 3 Nevada CoC

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

2.2 HMIS Oversight Inclusive Participation

Membership of the HMIS Working Group or advisory board is inclusive of decision makers representing the three Nevada CoCs and community.

Responsible Party
3 Nevada CoC

2.3 HMIS IT Issue Monitoring (Community Level)

HMIS System service requests, activities, deliverables and resolutions are reviewed on a regular basis. When necessary, authoritative support is provided to expedite IT issue resolution.

Responsible Party
HMIS Lead oversees HMIS Administrator

2.4 HMIS Technical Support

Technical expertise that is commensurate with the general HMIS program oversight is provided in addition to timely support on high level technical matters. All necessary HMIS software changes in response to the changing requirements of participating agencies are reviewed and authorized. All general special issues presented by participating agencies are reviewed and authorized.

Responsible Party
HMIS Lead oversees HMIS Administrator

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

2.5 HMIS Software Technical Support

Technical expertise commensurate with the requirements of the HMIS software and/or system is provided; Timely support on software technical matters is provided; Authorized changes to the HMIS software and processes are implemented; Resolutions to any special issues authorized by the HMIS Technical Support Entity within the software and/or overall system are implemented.

Responsible Party
HMIS Lead oversees HMIS Administrator

2.6 HMIS IT Issue Tracking

An updated list of HMIS system service requests, activities, deliverables, and resolutions is maintained on a regular basis**.**

Responsible Party
HMIS Lead oversees HMIS Administrator

2.7 HMIS Staff Organization Chart

A current and accurate organization chart that clearly identifies all team members, their roles and responsibilities, and general work activities/functions is maintained on a regular basis. This organization chart is made available for review.

Responsible Party
HMIS Lead

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

2.8 HMIS Software Training

Regular training on software usage, software and data security, and data entry techniques to participating agencies is provided. The development, updating, and dissemination of data entry tools and training materials occur on a regular basis. The system is monitored and ensured on a regular basis.

User, Administrator And Security Training: Clarity Human Services will provide training to instruct the Clarity Nevada System Administrator in the proper procedures required to supervise and maintain the operation of the HMIS. System Administration training will cover security, configuration, and user customization.

Participating Agency Technical Administrator / Security Officer Training: Each agency participating in the Clarity Nevada system will designate a Technical Administrator / Security Officer who will serve as the contact person for participation in the HMIS. This person shall review and assess the security measures in place to protect client data.

Other responsibilities of this position include, but are not limited to, the following:

- Authorizing Agent For Partner Agency User Agreements
- Keeper Of Partner Agency User Agreements
- Keeper Of Executed Client Informed Consent Forms
- Authorizing Agent For User ID Requests
- Staff Workstations
- Internet Connectivity
- End User Adherence To Workstation Security Policies
- Detecting And Responding To Violations Of The Policies And Procedures
- First Level End User Support
- Maintain Agency/Program Data In HMIS Application
- Authorized Imports Of Client Data

Each organization participating in the Clarity Nevada system will have a representative participate in the Participating Agency Technical Administrator / Security Officer Training Program prior to system deployment at that agency. Training will take place

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

in Nevada, and participants are not to exceed fifteen persons per training. These trainings will cover practical problem solving. Each agency's Technical Administrator / Security Officer will learn how to adjust eligibility screens, identify service data that must be migrated to the HMIS, and track expenses and customize the system for their organization.

Each Participating Agency Technical Administrator / Security Officer will have access to a master manual for program management, and will be responsible for either copying or purchasing a copy for use at their organization. Upon conclusion of the training and prior to deployment, Technical Administrators / Security Officers will begin inputting their HMIS information, number of beds (if any), services, and contact information into the Clarity Nevada system.

End User Training Schedule: Bitfocus, Inc. will provide training in the day-to-day use of the Clarity Nevada system. Training class size will be limited. Training will use an established demo database, and will cover the following topics: intake, assessment, information and referral, reports, and client tracking. Training on any agency-modified fields/screens will be the responsibility of the associated agency making the modification. Training requires an eight to twelve hour commitment over the course of two days.

Responsible Party
HMIS Lead oversees HMIS Administrator

2.9 System Operation & Maintenance

Operation and maintenance of the HMIS System is conducted on a daily basis.

Responsible Party
HMIS Lead oversees HMIS Administrator

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

2.10 HMIS User Feedback

Mechanisms for soliciting, collecting, and analyzing feedback from end users, program managers, agency executive directors, and homeless persons are managed and maintained. Feedback includes impressions of operational milestones and progress, system functionality, and general HMIS operations. Examples of feedback include satisfaction surveys, questionnaires, and focus groups for all 3 Nevada CoC.

Responsible Party
HMIS Lead

3. HMIS Management & Operations: Compliance Monitoring

3.1 HMIS Management Issues

HMIS is managed in accordance to the policies, protocols, and goals of each of the three Nevada CoCs.

Responsible Party
HMIS Working Group and 3 Nevada CoC

3.2 HMIS Program Milestones Monitoring

Milestones, notes variances, and reports variances to CoC membership is monitored.

Responsible Party
HMIS Lead

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

3.3 Agency and Program HMIS Participation

Program- and agency-level participation in HMIS is monitored on a regular basis via the comparison of point-in-time census of beds/slots to clients served. Agencies report all findings to their corresponding Nevada CoC.

All monitoring activity is documented. Acceptable documentation methods can include but are not limited to the following reports: [DQXX-103] Monthly Staff Report; Monthly Agency Utilization Report; [HSNG-102] CoC Housing Assessment Report; [HSNG-103] Housing Inventory Report; Monthly Housing Report (both CoC- and Agency-based); Weekly Housing Census; Performance Monitoring Report(s).

Responsible Party
3 Nevada CoC

3.4 Data and System Security

Agency staff are instructed and required to adhere with the HMIS data and system security protocols as outlined by their corresponding CoC and the most current HUD HMIS Data and Technical Standards.

HMIS Security Standards:

- HMIS Lead must establish a security plan that is approved by the CoC
- HMIS Lead must designate a security officer
- HMIS Lead must conduct workforce security screening
- HMIS Lead must report security incidents
- HMIS Lead must establish a disaster recovery plan
- HMIS Lead must conduct an annual service review
- HMIS Lead must ensure that each CHO designates a security officer and conducts workforce security measures
- HMIS Lead must ensure that each user completes security training (at the minimum annually)

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

- HMIS Lead must ensure that each CHO conducts an annual security review

Responsible Party
HMIS Lead oversees HMIS Administrator

3.5 Client Consent

Client consent is obtained and documented according to the Client Consent Policies and Protocols of the given Nevada CoC.

Interagency Data Sharing Agreements: Agencies that will be sharing client specific records must agree in writing to uphold specified minimum standards of privacy protection.

Written Client Consent Procedure For Data Entry: Agencies must obtain the client's consent prior to entering information concerning a client into the system. If a client does not consent, services should not be denied to the client. The agency can use the anonymous client function in appropriate cases.

Confidentiality And Consent Forms: Agencies must use the forms approved by the HMIS Working Group. Agencies that share protected health information must have internal procedures for obtaining client consent prior to the sharing of this information.

Privacy Notice: Agencies must develop a privacy notice, and incorporate the Clarity Privacy Notice into its policies and procedures. In addition, HUD mandates that organizations develop policies and procedures to distribute privacy notices to their employees, which include having employees sign to acknowledge receipt of the notices.

Responsible Party
Participating Agency

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

4. HMIS Management & Operations: Data Quality

4.1 Data Quality Standards

Community level data quality plan and standards are developed and enforced. A standard interview protocol that facilitates the collection of required data elements is developed. These standard interview protocols include standardized intake as well as standardization of all subsequent interviews.

Data Quality Standards:

- HMIS Lead must set data quality benchmarks for CHOs separately for lodging and non-lodging projects.
- Minimum Bed Coverage Rates: Measures the level of lodging project providers' participation in HMIS. Must be calculated separately for emergency shelter, safe haven, transitional housing, and permanent housing.
- Divide the number of HMIS participating by the total number of year-round beds in the CoC geographical area.
- Service-Volume Coverage Rates: Service-Volume coverage rate will all calculation of the coverage rate for a HUD-defined category of projects that do not offer overnight accommodations, such as homelessness prevention projects or street outreach projects. Must be calculated for each comparable database.
- Divide the number of persons served annually by the projects that participate in the HMIS by the number of persons served annually by all CoC projects within the HUD-defined category.
- All HMIS Leads must develop and implement a Data Quality Plan. HMIS must be able to generate reports monitoring data quality.

HMIS Leads and CHOs must refer to applicable program regulations in regards to the length of time records are to be maintained and monitored. While the HMIS

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Lead is permitted to archive the data in HMIS, they must follow HUD archiving data standards.

Responsible Party
HMIS Lead and 3 Nevada CoC

4.2 Universal Data Elements

Data quality reports are regularly reviewed at community planning level. These data quality reports generate information that covers data entry completion, consistency with program model, and timeliness as compared to the community data quality standards. All standardized interview protocol adhere to the requirements outlined in the most current HUD Data Standards.

The Universal Data Elements outlined in the most current HUD Data Standards will be collected and/or verified per HUD procedure at initial intake and any subsequent program enrollment, and then entered into the HMIS within a specified period of time following the collection of the data.

Responsible Party
Participating Agency and 3 Nevada CoC

4.3 Program Specific Data Elements

The collection of each data variable and corresponding response categories specific to their program type on all clients served by McKinney-Vento funding is ensured. All standardized interview protocol prescribed by HUD is followed.

The Program-Specific Data Elements are collected and/or verified per HUD procedure at initial intake and any subsequent program enrollment, and then entered into the HMIS within a specified period of days from the collection of the data.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Reporting agencies are required to report program entry and exit dates upon the entry or exit of program participants. Entry dates should record the first day of service or program entry with a new program entry date for each period/episode of service. Exit dates should record the last day of residence in a program's housing before the participant leaves the shelter or the last day a service was provided.

Responsible Party
Participating Agency and 3 Nevada CoC

4.4 Data Quality Reports – Technical Assistance

Data quality reports that indicate levels of data entry completion, consistency with program model, and timeliness as compared to the community data quality standards are disseminated to participating programs. Technical assistance and training needs are determined according to these reports.

Responsible Party
HMIS Lead oversees HMIS Administrator

4.5 Data Quality Reports to Planning Entity

Data quality reports that indicate cross program levels of data entry completion, consistency with program model, and timeliness as compared to the community data quality standards are disseminated to the three Nevada CoC on a regular basis.

Responsible Party
Participating Agency and 3 Nevada CoC

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

4.6 Meta Data Elements

Meta Data Elements are defined as elements of information that describes an item; they are not the item itself. Meta Data Elements do not actually appear on the screen, but instead describe the data fields that do appear on the screen. Thus, Meta Data Elements are an integral and automated component of the data collection process. All meta data elements adhere to the requirements outlined in the most current HUD Data Standards.

Requirements: Each data variable and corresponding response categories specific to their program type on all clients served by McKinney-Vento funding are collected through proper data collection. All standardized interview protocol adheres to the most current HMIS requirements. Therefore, the Meta Data Elements are collected and/or verified per HUD procedure at initial intake and any subsequent program enrollment, and entered into the HMIS within a specified period of time following the collection of the data.

Responsible Party
Participating Agency and HMIS Administrator

5. HMIS Policy Development & Oversight

5.1 Community Planning Goals & Objectives Training

The progress of the Community Planning Goals and Objectives trainings and reviews are monitored on a regular basis.

Responsible Party
3 Nevada CoC

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

5.2 Participation Rates

HMIS coverage rates of the three Nevada CoCs are reviewed and monitored on a regular basis. Agencies with coverage rates lower than 75% participation are required to provide explanation for the barriers to implementation. Ongoing engagement activities and barrier resolution with non-participating agencies is required.

Responsible Party
HMIS Lead and 3 Nevada CoC

5.3 Client Confidentiality & Privacy Training

Training on client confidentiality and privacy requirements are provided to intake staff, data entry staff, and reporting staff at all participating agencies on a regular basis. All agencies have sufficient privacy policies and protocols in place.

Responsible Party
HMIS Administrator

5.4 Performance Measurement Training

Regular training and guidance on program performance measurement is provided.

Responsible Party
HMIS Lead oversees HMIS Administrator

5.5 Participating Agency Documentation

The number of participating agencies (utilizing the system) is maintained and documented on a regular basis for all 3 Nevada CoC. A comparative analysis of

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

planned versus actual deployments at the project level is highly desired but not compulsory.

Responsible Party
HMIS Lead

5.6 Policies & Procedures

HMIS Policies and Procedures are fully documented and available.

Responsible Party
HMIS Lead

5.7 Agency Participation Agreement

Written agreements that describe the protocols for participation in the HMIS are established with participating agencies.

Responsible Party
HMIS Lead

5.8 Data Sharing Agreements

Written agreements with participating agencies who share client level data are maintained. These agreements describe the level of data element or program information sharing among the data sharing HMIS agencies.

Sharing Of Information: Clients must consent to the sharing of their information prior to that information being shared with participating agencies. In the event that the client agrees to have their information entered into the HMIS, but does not agree to have it shared with other agencies, the user can make the client record anonymous by using the 'Private Option'.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Sharing Protected Information: A separate Release of Information (ROI) indicating what information the client agrees to have shared with other participating agencies must be signed prior to sharing of any Protected Personal Information (PPI).

Printed Information: Any printed records that are disclosed to the client or another party should indicate: the person and/or agency to whom the record is directed, the date, and the initials of the person making the disclosure.

Requests For HMIS Client Information: The agency must notify the HMIS Program Administrator within one working day when the agency receives a request from any individual or outside organization for client-identifying information.

Case Notes: It is understood that client case notes will not be shared, and that each agency will have the ability to enter its own private notes about a client.

The Release of Information (ROI) form will be a dated document that expires. The provider will only be able to access the information specified on the ROI that was entered into the system during the time the ROI was in effect. Also, the client can decide at any time that they want to have their information closed, in full or in part, and/or client file deactivated.

Responsible Party
HMIS Lead with leadership from HMIS Working Group

5.9 HMIS End-User Agreement

A written agreement with each authorized user of the HMIS is maintained. This agreement defines participation protocols, including training criteria, consent protocols, system use, and privacy and security standards.

Responsible Party
HMIS Lead oversees HMIS Administrator

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

5.10 Data Release

The CoC and/or implementing jurisdiction geography (i.e. CoC geographical area) of the HMIS grantee maintains a defined and documented HMIS data release protocol that governs release of all data from the HMIS.

Responsible Party
HMIS Lead and/or HMIS Working Group and 3 Nevada CoC

5.11 Client Consent

The CoC and/or implementing jurisdiction geography (i.e. CoC geographical area) of the HMIS grantee have a defined and documented client consent protocol to be used as a baseline practice among all participating HMIS users.

Responsible Party
3 Nevada CoC

5.12 Program Funding Training & Orientation.

All required Clarity Nevada participants pertaining to HMIS standards (including McKinney-Vento funded programs such as CoC, ESG, and HOPWA projects that target homelessness) receive training and orientation on regulations pertaining to HMIS data collection.

Responsible Party
HMIS Administrator and 3 Nevada CoC

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

6. Other Federal Requirements

6.1 Drug-Free Workplace

The HMIS Grantee adopts and enforces a drug-free workplace policy. The policy is posted and available for review.

Responsible Party
HMIS Lead

6.2 Conflict of Interest

The HMIS Grantee adopts a conflict of interest policy for board members, staff, and volunteers.

Responsible Party
HMIS Lead

6.3 Equal Opportunity & Non-Discrimination Policy

The HMIS Grantee adopts an equal opportunity and non-discrimination policy.

Responsible Party
HMIS Lead

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

GLOSSARY

This section provides HUD definitions for terms commonly used throughout this document.

Clarity Nevada: This term refers to the implementation of the Clarity Human Services software as the statewide HMIS for Nevada.

Clarity System: This term refers to the Clarity Human Services HMIS software.

Client: A living individual about whom a Contributory HMIS Organization (CHO) collects or maintains protected personal information: (1) because the individual is receiving, has received, may receive, or has inquired about assistance from a CHO; or (2) in order to identify needs, or to plan or develop appropriate assistance within the CoC.

Continuum of Care (CoC): The primary decision making entity defined in the funding application 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.

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

Contributory CoC Program: A homeless assistance program or homelessness prevention program that contributes Protected Personal Information (PPI) or other client- level data to an HMIS.

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

Data Recipient: A person who obtains PPI from an HMIS Lead Agency or from a CHO for research or other purposes not directly related to the operation of the HMIS, CoC, HMIS Lead Agency, or CHO.

End User (or 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 in the HMIS or another administrative database from which data are periodically uploaded to the HMIS.

HMIS Lead Agency: An organization designated by a CoC to operate the CoC's HMIS on its behalf. Entity responsible for soliciting, collecting, and analyzing feedback from end-users, program managers, agency executive directors, and homeless persons.

HMIS Software Solution Provider: An organization that sells, licenses, donates, builds or otherwise supplies the HMIS user interface, application functionality and database.

HMIS User Committee: Group of entities that provide recommendations on use of software and software enhancements

HMIS Vendor: A contractor who is paid to provide services for the operation of a CoC's HMIS. An HMIS vendor includes an HMIS software solution provider, web server host, and data warehouse provider, as well as a provider of other contracted information technology or support.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Homeless Assistance Program: A program whose primary purpose is to meet the specific needs of people who are literally homeless (as defined in data element 3.11, Housing Status). Homeless assistance programs include outreach, emergency shelter, transitional housing, rapid re-housing, permanent housing and permanent supportive housing.

Homelessness Prevention Program: A program whose primary purpose is to meet the specific needs of people who are imminently losing their housing or at risk of losing their housing (as defined in data element 3.11, Housing Status.).) Homelessness prevention programs include those funded by HPRP and other homelessness prevention programs identified by the CoC as part of its service system.

Homeless Management Information System (HMIS): The information system designated by a CoC to process Protected Personal Information (PPI) and other data in order to create an unduplicated accounting of homelessness within the CoC. An HMIS may provide other functions beyond unduplicated accounting.

Nevada CoC Structure: The state of Nevada has three separate Continuums of Care. Although these CoCs operate independently in regards to services and programs, each utilizes the Clarity Nevada HMIS and the three CoCs collaborate on all matters regarding the Clarity Nevada HMIS.

Non-Contributory CoC Program: A CoC Program that does not contribute PPI or other client-level data to an HMIS.

Participating CoC Program/Agency: A Contributory CoC Program or Agency that makes reasonable efforts to record all the universal data elements and all other required data elements as determined by HUD funding requirements on all clients served and discloses these data elements through agreed upon means to the HMIS Lead Agency at least once annually.

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, taking into account any methods reasonably likely to be used, be learned by linking the information with other available information or by otherwise manipulating the information.

Processing: An operation or set of operations performed on PPI, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission and destruction of the PPI.

Technical Administrator / Security Officer: This person is designated by each agency to serve the following roles: primary contact for communications regarding HMIS; supervise software implementation; responsible for ensuring compliance with applicable security standards; organize and schedule timely new user set-up and end user training; run package reports; collaborate with HMIS lead in the development of customized reports; review and assess the security measures in place to protect client data.

Unduplicated Accounting of Homelessness: An unduplicated accounting of homelessness includes measuring the extent and nature of homelessness (including an unduplicated count of homeless persons), utilization of homelessness programs over time, and the effectiveness of homelessness programs.

Unduplicated Count of Homeless Persons: An enumeration of homeless persons where each person is counted only once during a defined period of time.

Victim Service Provider: A nonprofit or nongovernmental organization including rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

REFERENCES

[1] National Coalition for the Homeless. (2006) Fact Sheet #18: McKinney-Vento Act. Retrieved December 13, 2013 from: http://web.archive.org/web/20071203073025/http://www.nationalhomeless.org/ publications/facts/McKinney.pdf

[2] U.S. Department of Housing & Urban Development, Office of Community Planning and Development, Office of Special Needs Assistance Programs. (2001) Report to Congress: HUD's Strategy For Homeless Data Collection, Analysis and Reporting. Retrieved December 13, 2013 from: http://archives.hud.gov/offices/ cpd/homeless/hmis/strategy/congressreport.pdf

[3] U.S. Department of Housing & Urban Development, Office of Community Planning and Development. (2004) Third progress report to congress on HUD's strategy for improving homeless data collection, reporting, and analysis. Retrieved December 13, 2013 from http://archives.hud.gov/offices/cpd/homeless/hmis/strategy/reporttocongress2004.pdf

[4] "Homeless Management Information Systems (HMIS); Data and Technical "Standards Final Notice; Notice" Federal Register 69 (30 July, 2004): 45888-45934. Print.

[5] U.S. Department of Housing & Urban Development, Office of Community Planning and Development. (April 2017) 2017 Homeless Management Information Systems (HMIS) Data Dictionary. Retrieved April 2017 from: https://www.hudexchange.info/resource/3824/hmis-data-dictionary/

[6] "Homeless Management Information Systems Requirements, Proposed Rule." Federal register 76 (9 December, 2011): 76917-76927. Print.

CLARITY
HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT A

Participation Agreement

The signatures of the parties indicate their agreement with the terms and conditions set forth in this document.

By_____

Name

Title

By_____

Name

Title

By_____

Name

Title

By_____

Name

Title

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT B

Client Consent Revocation

The signatures of the parties indicate their agreement with the terms and conditions set forth in this document.

Clarity - Homeless Management Information System

Client Revocation of Consent to Release Information

I hereby revoke permission for the partner agencies in the Nevada Continuums of Care to share my personal information and information regarding my family in the Homeless Management Information System (HMIS). I understand that my information will remain in HMIS as part of the non-identifying data collected on homeless services provided by the Continuums of Care, but that my personal and family information will no longer be available to any partner agency.

_____ _____ _____
Client Name (please print) Client Signature Date

_____
Client HMIS Number

Executed At:

_____
Name of Partner Agency

_____ _____ _____
Agency Personnel Name (print) Agency Personnel Signature Date

Comments:
(Comments and ideas from clients and case workers are encouraged):

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT C

Client Information Sheet

Clarity - Homeless Management Information
Client Information Sheet

What is the HMIS System?
It is a networked, computerized record keeping system. HMIS stands for Homeless Management Information System, and is a requirement for all programs and agencies providing services to low-income and homeless households with the support of federal funds.

What is the purpose of the HMIS System?
The HMIS is used by provider agencies to record information about clients that they serve. This information helps the agencies plan for and provide services to clients. This information also can be shared among partnering agencies – in order to improve the coordination and delivery of your services. Partnering agencies have signed agreements to treat your information in a professional and confidential manner.

Why is this type of information being collected?
A summary of the information gathered from clients will be used to advocate for more adequate resources for homeless people. Gathering certain basic information (race, date of birth, family size, etc.) about you and the members of your household is also a requirement of the federal and local funding which supports this program.

How can the HMIS System benefit me, the client?
By gathering this information on you only once –you can be served by other agencies without reporting all the details (date of birth, social security number, last address, etc.) again and again. If there is a reason that providing your name or the name of other members of your household would place you (or your household member) at risk, then you can request that your information NOT be shared with other agencies. You have the right to revoke the sharing of your information at any time simply by completing a "Client Revocation of Consent to Release Information" form. This form is available at any HMIS-participating agency.

Also, by using the information you provide for the HMIS, you and your case worker can work together to identify the services you need and work to obtain them.

Who has access to your information?
Only approved, participating providers, or those who have administrative responsibilities in this HMIS will be authorized to look at, enter, or use information that is kept in your file. Report developers and Bitfocus staff may also see your data. There are strict guidelines for who has access to your information. Homeless advocates, shelter staff, and local, state, and federal officials will use non-Identifying client data to better address the needs of the homeless.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

What are your rights as a client?
You may be required to answer some questions as a prerequisite for a program, but there will be other questions you can choose not to answer. You have a right to view your record and to correct inaccurate information. You also have a right to a copy of your record. We will also NEVER give any information (health, medical needs, mental health, domestic violence, etc.) about you to anyone outside of the HMIS, UNLESS YOU GIVE WRITTEN CONSENT, or as required by law through a subpoena or a court order. If you choose to not answer any questions, you may not be able to receive services from this community.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT D

Client Privacy Statement

BITFOCUS INC.
HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

PRIVACY STATEMENT

YOU HAVE THE RIGHT TO REFUSE TO ANSWER ANY QUESTION COLLECTED FOR THE PURPOSE OF HMIS DATA COLLECTION

Agencies participating in the HMIS may ask and require some information from you as a part of regular program eligibility and services they provide. This information will be entered into the HMIS database. You are not required to answer any question asked for the sole purpose of HUD HMIS Data collection and you will not be denied services for refusing to answer the HUD HMIS data collection questions, unless specifically required for program eligibility.

Why We Collect Information

We collect personal information directly from you for reasons that are discussed in our Privacy Notice. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Additional personal information that we collect is important to run our programs, to improve the services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.

The collection and use of your personal information is guided by strict standards of confidentiality. Our Privacy Notice is posted. A copy of our Privacy Notice is available to all clients upon request.

HMIS PARTNER AGENCY USE OF YOUR INFORMATION
Purpose of Data Collection
Information you provide to this agency will be entered into Clarity Human Services, the Homeless Management Information System (HMIS). You will receive the same services, whether

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

or not you allow your additional personal information, as described below, to be shared with other Participating Agencies in the HMIS database.

- To provide, improve and/or coordinate services to individuals or families that could benefit for such services;
- For the administrative functions of these programs;
- To provide accurate reporting, as required by law or by the organizations that provide money for these programs, with aggregate data that has removed any identifying information;
- Your personal information that is in HMIS will not be shared with any government agencies without your knowledge or consent, except as required by law.

What information is collected about you?

The following personal information is shared with Participating Agencies within HMIS: Name; Photograph; Social Security Number; Date of Birth; Race; Ethnicity; Gender; Veteran Status; Chronic Homeless Status; Disabling Condition (Y/N) Status; Residence Prior to Program Entry; Zip Code of Last Permanent Address; Housing Status; Program Entry Date; Program Exit Date; Personal Client Identification Number; Household; and Household Identification Number.

Depending on your situation, you may be asked for some or all of the following:

The following additional personal information will not be shared with Participating Agencies without your consent: Agency Name(s) that provided you service(s); Income and Sources; Non-Cash Benefits; Physical Disability; Developmental Disability; Chronic Health Condition; HIV/AIDS; Mental Health; Substance Abuse; Domestic Violence; Destination; Date of Contact; Date of Engagement; Financial Assistance; Housing Relocation & Stabilization Services Provided; Employment; Education; General Health Status; Pregnancy Status; Veteran's Information; Children's Education; Reason for Leaving; Emergency Contact; and Services Provided.

YOUR RIGHTS & CHOICES:
What happens to your information?

- When you request services from this agency, your information will be entered into the Clarity Human Services HMIS, which operates over the Internet. HMIS uses many security protections to ensure confidentiality and only agencies that use the Clarity Human Services HMIS can access this program.
- Agencies participating in the HMIS may ask and require some information from you as a part of regular program eligibility and services they provide. This information may be entered into the HMIS database. You are not required to answer any questions asked for the sole purpose HUD HMIS Data collection and you will not be denied services for refusing to answer the HUD HMIS data collection questions, unless specifically required for program eligibility.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

- You have the right to change your mind about sharing your additional personal information. You must notify this agency in writing if you have changed your mind about sharing.

COMPLAINT PROCESS:

To file a complaint, please contact Bitfocus, Inc. – Nevada HMIS Administrator

nevada@bitfocus.com

T: 702.614-6690 x2
TF: 800.594.9854

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT E

Client Consent for Release of Information

Nevada Homeless Management Information System
Client Consent for
Data Collection and Release of Information

What is the HMIS?
The HMIS is a data system that stores information about homelessness services. Bitfocus, Inc. manages the HMIS for the state of Nevada. The purpose of the HMIS is to improve services that support people who are homeless or at risk of homelessness to get housing, and to have better access to those services, while meeting requirements of funders such as the U.S. Department of Housing and Urban Development (HUD).

What is the purpose of this form?
With this form, you can give permission to have information about you collected and shared with Partner Agencies that help Nevada provide housing and services. A current list of Partner Agencies is available at http://nvcmis.bitfocus.com/.

BY SIGNING THIS FORM, I AUTHORIZE the state of Nevada and Bitfocus to share HMIS information with Partner Agencies. The HMIS information shared will be used to help me get housing and services. It will also be used to help evaluate the quality of housing and service programs. I understand that the Partner Agencies may change over time.

The information to be collected and shared includes:
- Name, date of birth, gender, race, ethnicity, social security number, phone number, address
- Basic medical, mental health, substance use, and daily living information
- Housing Information
- Use of crisis services, veteran services, hospitals and jail
- Employment, income, insurance and benefits information
- Services provided by Partner Agencies
- Results from assessments
- My photograph or other likeness (if included)

BY SIGNING THIS FORM, I UNDERSTAND THAT:
- Bitfocus and Partner Agencies will keep my HMIS information private using strict privacy policies. I have the right to review their privacy policies.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

- I can receive a copy of this Consent and the Client Information Sheet
- I may refuse to sign this Consent. If I refuse, I will not lose any benefits or services.
- This Consent will expire 7 years from my last HMIS recorded activity.

I may revoke this Consent earlier at any time by returning a completed Revocation of Consent form, available at http://nvcmis.bitfocus.com/, to nevada@bitfocus.com.

- The revocation will take effect upon receipt, except to the extent others have already acted under this Consent.
- My HMIS information may be viewed by auditors or funders who review work of the Partner Agencies, including HUD, The Department of Veteran Affairs, and The Department of Health and Human Services. I understand that the list of auditors and funders may change over time.
- My HMIS information may be shared to coordinate referral and placement for housing and services.
- My HMIS information may be further shared by the Partner Agencies to other agencies for care coordination, counseling, food, utility assistance, and other services.
- My HMIS information will be used to help evaluate the quality of social services.
- My HMIS information may be used for research; however, my identity will remain private.

SIGNATURE:

_____ _____
Signature of Patient/Client or Representative Date

_____
PRINTED NAME

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT F

Client Grievance Form

Client Grievance Form
Instructions

HMIS Clients are encouraged to work with the agency they are having issues with before submitting a grievance. A grievance should be used as a last resort. All grievances are taken VERY seriously, and reviewed by the HMIS Working Group on an individual basis.

If you have not been able to resolve your issue with the agency directly, please complete the attached form.

- **Complete ALL fields**
- **Print Legibly**
- **Be as specific and as detailed as possible**
- **Attach additional pages as necessary**
- **Sign and Date the form**

After you have completed the form, please deliver the form to Bitfocus, Inc. at nevada@bitfocus.com or contact 702-614-6690 ext.2 for assistance.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

State of Nevada
Homeless Management Information System
Client Grievance Form

Client Name:

Agency Name: *List the agency you have been working with to solve this issue.*

Agency Contact Person: *List the name and phone number of the person you have been working with to solve the issue.*

First Date of Problem: *List the date you first began working on this issue.*

Description of Issue: *Please use the space below to describe your issue. Please print legibly and be as detailed as possible. Attach additional pages as needed.*

Please sign and date below:

_____ _____

Client Signature *Date*

Version2.0 *This form may not be amended except on approval of the*
Version Date: 2015/11 *HMIS Working Group.*

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT G

User Policy & Responsibility Statement

CLARITY - STATE OF NEVADA HOMELESS MANAGEMENT INFORMATION SYSTEM
USER POLICY AND RESPONSIBILITY STATEMENT - CODE OF ETHICS

_____
Name

_____
Email

_____
Phone #

Section 1 – Authorization to attend training.
The agency must complete section 1 and the user must attend User Training with Bitfocus, Inc., the Nevada State HMIS Administrator.

The person listed above is an employee or volunteer in good standing with our agency, and is approved by our agency as an authorized user.

_____
Agency Name

_____ _____
Agency Authorized Signature Date

Section 2 – User Policy, Responsibility & Code of Ethics.
This section must be completed by the user and turned in to the system administrator to complete the creation of a user account.

User Policy
Participating agencies shall share information for provision of services to their clients through a networked infrastructure that establishes electronic communication among the participating agencies.

Participating agencies shall at all times have rights to the data pertaining to their clients that was created or entered by them in the Nevada HMIS. Participating agencies shall be bound by all restrictions imposed by clients pertaining to the use of personal data.

It is a client's decision about whether or not to have his or her information entered into the HMIS system and shared with participating agencies. The client must sign a release consenting to the sharing of information.

The Nevada HMIS contains public alert functionality to bring specific client level information to the immediate attention of any user accessing a client record. Data shared within a public alert posting is meant to notify providers of pertinent information necessary or helpful to assist with the provision of services and should never be used to discriminate or cause harm to a client. Questionable information, as pertains to the public alert system, should be brought to the attention of the system administrator for possible removal.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Data necessary for the development of aggregate anonymous reports of homeless services, including services needed, services provided, referrals, client goals and outcomes should be entered to the greatest extent possible.

The Nevada HMIS system is a tool to assist agencies in focusing services and locating alternative resources to help homeless persons. Therefore, agency staff should use the client information in the Nevada HMIS to target services to their clients needs.

User Responsibility
Your User ID and Password give you access to the Nevada HMIS. Initial each item below to indicate your understanding and acceptance of the proper use of your User ID and Password. Failure to uphold the confidentiality standards set forth in the Nevada HMIS Standard Operating Procedures is grounds for immediate termination from the Nevada HMIS system.

_____ My User ID and Password are for my use only and must not be shared with anyone.

_____ I must take all reasonable means to keep my Password physically secure.

_____ I understand that the only individuals who have the right to review information in the Clarity Nevada system are authorized users and the clients to whom the information pertains.

_____ I may only view, obtain, disclose, or use the database information that is necessary to perform my job.

_____ If I am logged into the Clarity Nevada HMIS and must leave the work area where the computer is located, I must log off the Clarity Nevada system before leaving the work area.

_____ A computer that has the Clarity Nevada HMIS "open and running" shall never be left unattended.

_____ Failure to log off the Clarity Nevada HMIS appropriately may result in a breach in client confidentiality and system security.

_____ Hardcopies of data from the Clarity Nevada HMIS must be kept in a secure file.

_____ When hardcopies of data from the Clarity Nevada HMIS are no longer needed, they must be destroyed to maintain confidentiality.

_____ If I notice or suspect a security breach, I must immediately notify the agency administrator or the system administrator.

_____ I understand that I must complete confidentiality and privacy training on an annual basis. Failure to do so will result in the expiration of my User ID and Password.

_____ I understand that I may be subject to disciplinary action in accordance with my agency's Policies & Procedures if I fail to comply with this User Agreement.

User Code of Ethics

A. The Clarity Nevada HMIS users must treat participating agencies with respect, fairness, and good faith.

B. Each Clarity NevadaHMIS user should maintain high standards of professional conduct in his or her capacity as a system user.

C. Each Clarity Nevada HMIS user has a primary responsibility for his or her client(s).

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

D. Each Clarity Nevada HMIS user has the responsibility to relate to the clients of other participating agencies with full professional consideration.

I understand and agree to comply with all the statements listed above.

_____	_____
Printed Name	Email Address / Phone #
_____	_____
User Signature	Date

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT H

HMIS Disaster Recovery Plan

>>PLEASE SEE FOLLOWING PAGES<<

CLARITY
HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Information Security Department

DISASTER RECOVERY PLAN

Summary Plan

Purpose: One of the objectives of Bitfocus, Inc. information security department is to establish an IT Disaster Recovery Plan. This Disaster Recovery Plan document was created to assist Bitfocus, Inc. in the development of consistent and cohesive IT Disaster Recovery Plans.

This is a summary document which omits key infrastructure references to protect our our Information Security Infrastructure.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Introduction

The purpose of this summary is to document a Disaster Recovery Plan that addresses information resources as they may be affected in the event of a disaster. This document is meant to minimize any of these effects, and enable Clarity Human Services to either maintain, or quickly resume, mission-critical functions. This Disaster Recovery Plan also serves as the primary guide for Bitfocus, Inc. Information Technology Services Department in the recovery and restoration of the information technology systems in the event that they are damaged or destroyed as a result of a disaster.

Document Overview

The Disaster Recovery Plan is composed of numerous sections documenting the resources and procedures to be used in the event that a disaster occurs at the data center, which is located at Viawest in Las Vegas, Nevada. Separate sections are devoted to the specific recovery procedures for each supported application or platform. Also included are sections documenting the personnel requirements that are necessary to perform each recovery task. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Due to the very sensitive nature of the information contained in the plan, this summary omits several key references.

PERSONNEL AUTHORIZED TO DECLARE A DISASTER OR RESUME NORMAL OPERATIONS

Name	Title
Robert Herdzik	President & CEO
Tauri Royce	Project Manager

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Disaster Recovery Plan Summary

Plan Activation

This plan will be activated in response to internal or external threats to the Information Technology Systems of Bitfocus, Inc. Internal threats could include fire, bomb threat, loss of power or other utility or other incidents that threaten the staff and/or the facility. External threats include events that put the facility in danger. Examples might include severe weather or a disruptive incident in the community. Once a threat has been confirmed, the plan management team will assess the situation and initiate the plan if necessary.

Resumption of Normal Activities

Once the threat has passed, equipment will be repaired and/or replaced, and/or a new data center will be transitioned. The disaster recovery team will then assess the situation; If the disaster has expired, the team will resume normal operations.

Plan Objectives

The primary objectives of this plan are to protect Bitfocus, Inc. resources, to safeguard the vital records of which Clarity Human Services is the custodian, and to guarantee the continued availability of essential IT services. The role of this plan is to document the pre-agreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the data center and its services.

A disaster is defined as the occurrence of any event that causes a significant disruption in IT capabilities. This plan assumes the most severe disaster, the kind that requires moving computing resources to another location. Less severe disasters are controlled at the appropriate management level as outlined in this plan.

The basic approach, general assumptions, and possible sequence of events that need to be followed are stated in the plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The plan is a roadmap from disaster to recovery. Due to the nature of the disaster, the steps outlined may be skipped or performed in a different sequence. The general approach is to make the plan as threat independent as possible. This means that it should be functional regardless of what type of disaster occurs.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

For the recovery process to be effective, the plan is organized around a team concept. Each team has specific duties and responsibilities once the decision is made to invoke the disaster recovery mode. The leader of each team and their alternates are key personnel. IT staff will be assigned to multiple teams with specific assignments made according to knowledge, experience and availability. It is also assumed vendors and knowledgeable personnel will be actively enlisted to help during a recovery situation.

The plan represents a dynamic process that will be kept current through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognized, the plan will be revised to reflect the current IT environment.

Disaster Recovery Phases

The disaster recovery process consists of four phases. They are:

Phase 1: Disaster Assessment
Phase 2: Disaster Recovery Activation
Phase 3: Alternate Site/Data Center Rebuild
Phase 4: Return Home

Phase 1: Disaster Assessment

The disaster assessment phase lasts from the inception of the disaster until it is under control and the extent of the damage can be assessed. Cooperation with Viawest emergency personnel is critical.

Phase 2: Disaster Recovery Activation

This phase begins if the decision to move primary processing to a location is made. The Disaster Recovery Management Team will assemble at the command center and call upon team members to perform their assigned tasks. The most important function is to fully restore operations at a suitable location and resume normal functions. Once normal operations are established at the alternate location, Phase 2 is complete.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Phase 3: Alternate Site Operation/Data Center Rebuild

This phase involves continuing operations at the alternate location. In addition, the process of restoring the primary site will be performed.

Phase 4: Return Home

This phase involves the reactivation of the primary data center at either the original or possibly a new location. The activation of this site does not have town be as rushed as the activation of the alternate recovery center. At the end of this phase, a thorough review of the disaster recovery process should be taken. Any deficiencies in this plan can be corrected by updating the plan.

Key Disaster Recovery Activities

Declaring a Disaster

Declaring a disaster means:

2. Activating the recovery plan
3. Notifying team leaders & staff
4. Notifying key management contacts
5. Notifying affected customer contacts
6. Securing a new location for the data center
7. Ordering and configuring replacement equipment
8. Reconfiguring the network
9. Restoring Virtual Machine infrastructure from onsite or offsite Backup
10. Keeping management informed
11. Keeping customer contacts informed

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Disaster Decision Tree

Event	Decision
Data Center destroyed	Activate disaster recovery plan
Data Center unusable for MORE than 2 days	Activate disaster recovery plan
Data Center unusable for 2 days or LESS	Management Team perform an assessment
Network down	Management Team perform an assessment
Environmental problems (A/C, power, etc)	Management Team perform an assessment

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Decision Making For A Data Center Disaster

Decision Point	Actions				Category
1. Incident occurs	2. Alarm sounds	3. Begin evacuation	4. Ensure all employees evacuated	5. Meet in designated area	Initiation
7. Determine if incident is real	8. If no, then	9. Recovery plan is not activated	10. Return to normal operations	12. Evaluate evacuation	Determination
7. Determine if incident is real	8. If yes, then	9. Switch call handling to an alternate location			Determination
10. Determine scope of incident and assess damage after building access is allowed	11. If small scope with no to minimal damage, then	12. Return and begin clean up and monitor repairs	13. Return calls	14. Return to normal operations	Short Evacuation Required
10. Determine scope of incident and assess damage after building access is allowed	11. If moderate to large scope or moderate to severe damage, then	12. Activate alternate computer processing site	13. Activate recovery team	14. Notify management and employees of of situation	Moderate to Severe Damage to Data Center or Infrastructure
16. Assess damage	17. If damage is moderate and will be able to return in 30 days or less	18 Complete repairs as necessary while operating at alternate site	19. Return to data center	20. Return to normal operations	Moderate Severe Damage to Data Center or Infrastructure
16. Assess damage	17. If more than 30 days, locate to new facility	18. Order supplies and equipment	19. Set up and operate at new facility while completing repairs	20. Return to normal operations	Severe Data to Data Center or Infrastructure

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Recovery Time Objectives (RTO)

The Recovery Time Objectives reflect the estimated recovery times based on current configurations and operations.

NETWORK SERVICE	RECOVERY GOAL
LAN (Local Area Network)	2-3 days estimate
WAN (Wide Area Network)	2 days estimate
Internet	2 days estimate

APPLICATION RECOVERY TIER	RECOVERY GOAL
Infrastructure Servers	Immediately after WAN/Internet restore
Application / SQL Servers	3 days after LAN/WAN restore
Reporting Servers	5 days after LAN/WAN restore

These RTO's should be considered best-case estimates. Bitfocus, Inc. operates on a VMware virtual environment, with all server tiers fully virtualized. In the event of a disaster, the Disaster Assessment Team would assess the situation to determine if the local VM backups or the offsite VM backups (Amazon S3/Glacier) would be selected for recovery.

Once the assessment is complete, the Disaster Assessment Team will determine which temporary Data Center location to restore to. Current options are identified as Amazon Cloud or our Reno Data Center. Both locations are on standby.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Recovery Point Objectives (RPO)

Recovery Point Objectives (RPO) reflects the estimated point in time to which recovery would be made based on current configurations and operations. the exact recovery point for each server will vary due to the time when the backup takes place and when the disaster occurs. Below are general guidelines for the different types of DR data protection.

DATA PROTECTION TYPE	RECOVERY POINT (AGE OF DATA)
Onsite Backup	Up to 24 hours from disaster period.
Offsite Backup	Up to 7 days from disaster period.

Customers who have purchased additional Disaster Recovery SLA plans may have shorter RPO.

Roles of the Disaster Recovery Coordinator

The function of the Disaster Recovery Coordinator is vitally important to maintaining the plan in a consistent state of readiness. The Recovery Coordinator's role is multifaceted. Not only does the Coordinator assume a lead position in the ongoing life of the plan, but the Coordinator is a member of the Continuity Management Team in the event of a computer disaster.

The primary responsibilities of the Disaster Recovery Plan Coordinator are as follows:

- Distribution of the Disaster Recovery Plan
- Training the Disaster Recovery Teams
- Testing of the Disaster Recovery Plan
- Evaluation of the Disaster Recovery Plan Tests
- Review, change and update the Disaster Recovery Plan

In a disaster situation, the Disaster Recovery Plan Coordinator will:

- Facilitate communication between technical and non-technical staff
- Act as a Project Manager to coordinate the efforts of:
  - Technical Staff
  - Business Staff

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

- Vendors
- Other personnel as needed

The Disaster Recovery Coordinator for Bitfocus, Inc. is Robert Herdzik. The alternate Disaster Recovery Plan Coordinator is Yanis Guenane.

Overview of Offsite Storage

Items Stored Offsite

1. Router / VPN Firmware and Export Settings.
2. A current copy of this disaster recovery plan.
3. A copy of Veeam Backup & Recovery 7 extract utility.
4. Weekly backups of full VMware Virtual Machine files of entire infrastructure and data.

All standard security and privacy precautions apply to offsite storage. The offsite storage facility is equipped with surge protectors and natural disaster protective measures.

Onsite backup includes all of the above, including nightly full Virtual Machine incremental backups of entire infrastructure and data.

Server Recovery General Information

These procedures outline the steps required to restore any of Bitfocus, Inc. servers. Recovery for the servers assume that:

- Good backup data exists and can be retrieved from either onsite or offsite storage
- Replacement servers are on standby or Amazon Cloud servers are on standby
- Network connectivity is established

A decision must be made as to where the recovery will take place (Amazon Cloud or Reno Data Center). This decision is not made ahead of time since the specifics of the incident requiring recovery is not known.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Disaster Recovery Plan Maintenance

The disaster recovery plan is a "living" document. Failure to keep it current could severely impact Bitfocus, Inc. ability to successfully recover in the event of a disaster.

Some information contain in the plan is more dynamic than other information. A matrix of events and recommended maintenance schedule is included in this section. It is important to document changes to the plan and ensure that all copies of the plan are updated.

Changes to the plan could occur more frequently than the time frames listed in the following table. Major hardware upgrades might affect business recovery contracts as well as this plan. Software changes, personnel changes and other changes that affect the plan should be updated as soon as possible, not just when the recommended intervals occur.

PERIOD	ACTION
Quarterly	Review all job changes and update plan with new personnel assignments
Quarterly	Have any new application servers been implemented? If so, have all disaster recovery implication been addressed?
Quarterly	Have there been any major changes to existing applications? If so, update the recovery plan accordingly
Quarterly	Has the hardware configuration changed? If the changes affect your ability to recover, make appropriate changes to the recovery configuration.
Quarterly	Update the Network Configuration Diagrams / Infrastructure Wiki
Quarterly	Visit the off-site storage location and ensure documentation is available and current
Quarterly	Ensure all team assignments are still valid
Semiannually	Test the plan and update it based on the results of the test
Annually	Review Amazon S3 / Glacier retention requirements
Annually	Review Insurance coverage

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Testing the Disaster Recovery Plan

The Disaster Recovery Coordinator is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan. On an on-going basis this frequency appears to be adequate considering the systems involved. However, special tests are to be given consideration whether there has been a major revision to the plan or significant changes in the software, hardware or data communications have occurred.

The objectives of testing the disaster recovery plan are as follows:

- Simulate the conditions of an ACTUAL Business Recovery situation.
- Determine the feasibility of the recovery process.
- Identify deficiencies in the existing procedures.
- Test the completeness of the business recovery information stored at the Offsite Storage Location.
- Train members of the disaster recovery teams.

The initial test of the plan will be in the form of a structured walk-through and should occur within two months of the disaster recovery plan's acceptance. Subsequent tests should be to the extent determined by the Disaster Recovery Coordinator that are cost effective and meet the benefits and objectives desired.

Sample Recovery Test Agenda

1. What is the PURPOSE of the test?
2. What are the test OBJECTIVES?
3. How will the successful achievement of these objectives be measured?
4. At the conclusion of the test, collect test measurements from all participants.
5. Evaluate the test results. Determine if the test was successful or not.
6. Determine the implications of the test results. Does success for this test imply success in all recovery scenarios?
7. Update the plan based on results of the test.

CLARITY
HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT I

HMIS Security Plan

>>PLEASE SEE FOLLOWING PAGES<<

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Information Security Department

HMIS SECURITY PLAN

Purpose: The purposes of this HMIS Security Plan are as follows:

- Provide an overview of the security requirements of the Clarity Human Services HMIS application, and describe the controls in place or planned for meeting those requirements; and
- Delineate responsibilities and expected behavior of all individuals who access the system.

In accordance with the HMIS standards outlined by the U.S. Department of Housing and Urban Development, this Security Plan is to be reviewed and updated annually.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Introduction

Bitfocus Inc.

Bitfocus is a consultancy firm that provides the following HMIS Implementation services to the HMIS Lead Agency:

- HMIS Software and Server Administration
- Telephone Help Desk Support
- Ticket Support
- HMIS Implementation and Maintenance
- Remote Web Based and On-Site Training
- Remote Web Based and On-Site Technical Assistance
- Training Manual and Procedural Documentation
- Custom Report Writing
- Data Warehouse Development and Administration
- HMIS Working Group Meeting engagement
- Planning and Policy Making
- AHAR, APR, and QPR support

Bitfocus Inc. provides HMIS Administration services for:

- Northern Nevada Continuum of Care (CoC)
- Southern Nevada Continuum of Care (CoC)
- Balance of State Continuum of Care (CoC)

The Clarity Human Services HMIS Application

The Clarity Human Services HMIS Application is a cloud-based system that offers a comprehensive and end-user adjustable HMIS solution to meet the multiple integration, implementation, and management requirements of the state of Nevada Continuums of Care.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

General Description of HMIS Information Sensitivity

Clarity Human Services HMIS application stores and protects confidential individually identifiable health information. As such, it is equipped with a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

Applicable Laws Or Regulations Affecting The System

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA's Privacy Rule states that "Individually Identifiable Health Information" is to be considered "protected health information" [PHI] subject to the review and control of individual patients. Agencies and other entities handling PHI are mandated to restrict access to such information to appropriate persons and protect the privacy of individuals. Clarity Human Services includes customization features at micro and macro levels to automate the enforcement of federal, state, and local privacy requirements such as HIPAA.

Clarity Human Services Security Tools enable each partner agency to define which client data is shared with other agencies at every level, including the field level. The default data sharing setup associated with each partner agency can be defined on an agency-by- agency basis (i.e., Agency A may share all client data with Agency B, nothing with Agency C, and only core ID data with Agency D). Our privacy settings can be adjusted to override the default privacy configuration of each agency upon the request of the client.

Bitfocus, Inc. can confirm the capacity of Clarity Human Services to both meet and surpass current HIPAA & HUD requirements and the pending updates to the these requirements.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

HUD Homeless Management Information Systems Requirements

Bitfocus Inc. maintains operations that are in accordance with the most current HMIS Systems requirements as prescribed by the U.S. Department of Housing & Urban Development (HUD).

System Environment

The Clarity Human Services HMIS Application is a cloud-based system equipped with the following technical security features:

- **Hardware Firewall:** The firewall forwards only port 443 (Encrypted SSL) to the internal web server.
- **Software Firewall:** Each customer webserver on the internal network is also protected by a software firewall.
- **VPN Access:** Access to the internal network is only possible via an encrypted VPN connection. Access to the internal network is only provided to Clarity Human Services staff, and System Administrators, and our customers.
- **Database Server:** The database is housed on an internal server, inaccessible from the public network.
- **Encryption:** All traffic is 2,048 bit SSL encrypted. All API traffic must be further AES encrypted
- **PKI Encryption:** Customers may opt for staff or agency-level PKI encryption. Customers utilizing this method require an additional PKI certificate to be installed in their web browser to authenticate. PKI Certificates are fully administered within the System Administrator interface.
- **Encryption:** 2,048 bit SSL for all traffic
- **IP Whitelist**: Customers may opt for staff or agency level IP Whitelisting. Customers utilizing this method require each user to login from a System Administrator defined list of allowed IP Addresses

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

System Interconnection/Information Sharing

Role-Based Security

Clarity Human Services is designed around a sophisticated Access Control List (ACL) model, which provides granular level permissions to all areas of Clarity Human Services. The ACL was implemented using access roles. Individual access roles are assigned to a user to dictate which areas of the system they can view, what they can read/ write/edit or delete, and how those roles relate to agencies they are potentially sharing data with. The ACL was designed to be completely transparent to the end user. Any areas of the system to which they are denied access are eliminated from view, providing a seamless user experience on any access role.

Agency Sharing

If a participating agency wishes to share data through the HMIS with one or more other agencies:

1. All agencies wishing to share data must meet with Bitfocus to discuss and address all details of data sharing. For example: What information is to be shared, direction of sharing, etc.
2. A separate Memorandum of Understanding must be created between Bitfocus and all agencies that will participate in the inter-agency sharing.
3. Agencies must comply with Section 8 of this document (relating to obtaining clients' permission to have their information shared).

In regards to the coordination of data sharing, we are leaders in the field. Bitfocus partners with participating agencies and encourage them to sign Agency Data Sharing agreements, in order to allow for the coordination and management of shared service delivery. In Nevada, 98% of participating agencies have agreed to Agency Data Sharing Agreements.

Bitfocus has dedicated an entire section of the HMIS application to Agency Sharing. In this section, System Administrators can fine-tune their sharing settings with the ability to create Agency Sharing default settings as well as create any agency exceptions. They have the ability to control whether data categories have 'Not Shared', 'Basic Shared', and 'Full Sharing' settings. And, as mentioned, Agency Exceptions can be created

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Access Roles

In order to further protect client data during referral processes, Clarity Human Services has a section devoted to Access Roles. System Administrators have the ability to create different Access Roles, each with different capabilities. For example, if volunteers come to the agency just to do data entry, System Administrators can create an access role that allows these volunteers to view and modify only data necessary to their purpose. Different Access Roles can be customized to end users at the individual level

Intra- and Inter-Agency Restrictions

HIPAA requires entities sharing health data with each other to function within data-sharing protocols and agreements that support the basic principles of the HIPAA Privacy Rule. Clarity Human Services has sophisticated tools for assigning access rights to users. It is possible to define and create an unlimited number of Access Roles associated with varying levels of access down to every level, including the field level. Access Roles can also be defined on an agency basis. Each participating agency can define the data they wish to share with other organizations down to the field level. These cross-agency access rights can be adjusted on an agency-by-agency basis [e.g. Agency A may share all of its client data with Agency B, selected data with Agency C, and no data with Agency D]

Automated Audit Trail

Clarity Human Services provides complete auditing records on all areas connected to user interaction. The audit trails are accessible by two methods:

1. Log Link – On every page, a Log Link is presented at the bottom right of the screen. When the System Administrator selects this link, any updates made to any of the data presented on the screen will appear. Items such as Old Values, New Values, date/time of the update, and the user who made the update are all presented in a simple format.

2. Database – The audit log is also provided through the relational database, allowing the System Administrator to access the data using a Query tool, or write reports to manage the updates in any way the System Administrator defines

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Encryption Management

Encryption General

All information should be encrypted in the database per HUD standards. All connections to the Clarity database should be encrypted to HUD standards or higher. Encryption should be sufficient to prevent unauthorized personnel from accessing confidential information for any reason.

Encryption Management

In the event that system wide data decryption becomes necessary, the Working Group must obtain the written authorization of every participating agency's executive director.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

HMIS CONCEPTS & TERMS

Aggregate - Collected together from different sources and considered as a whole, and lacking identifying information.

Client - Somebody who uses or applies to use the services of a participating agency.

CoC – The acronym for Continuum of Care

Community - A group of people with a common background or with shared interests within a defined geographic area, for our area to include the state of Nevada.

Confidentiality - Entrusted with somebody's personal or private information or matters.

Connectivity – The ability to connect two or more systems together. Pertaining to the HMIS system, the use of a high speed Internet connection for accessing the system.

Consent – Express acceptance of or agreement to something.

Data – The information in the system, for example, numbers, text, images, and sounds, in a form that is suitable for storage in or processing by a computer

Decryption – To render an encoded amount of data into plain language or out of its encrypted state.

Encryption – To convert computer data and messages to something incomprehensible by means of a key, so that only an authorized recipient holding the matching key can reconvert it.

Firewall – A component of a network that prevents unauthorized users and/or data from getting in or out of the network, using rules to specify acceptable communication

HMIS – The acronym for Homeless Management Information Systems, sometimes also referred to as HIMS or Homeless Information Management System.

HUD – The acronym for the Department of Housing and Urban Development.

Legacy Data – Information stored in an older version of software or format that is not compatible with the HMIS system.

Clarity Human Services– The name of the software application that being used for the Nevada HMIS.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Clarity System – The name that has been given to our implementation of an HMIS system.

MOU – The acronym for Memorandum of Understanding. A document that outlines the specific areas of agreement between two or more parties.

Organization - A group of people identified by shared interests or purpose.

PPI – The acronym for Protected Personal Information.

Program – A collection of services grouped together.

ROI – The acronym for Release of Information.

Service - The system or operation by which people are provided with something.

VPN – The acronym for Virtual Private Network. A way for securely connecting systems together to transmit data.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT J

HMIS Data Quality Plan

>>PLEASE SEE FOLLOWING PAGES<<

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Information Security Department

HMIS DATA QUALITY PLAN

Purpose: The purposes of this HMIS Data Quality Plan are as follows:

- Identify the responsibilities of all parties within the CoC that affect data quality.
- Establish specific data quality benchmarks for timeliness, completeness, and accuracy.
- Describe the procedures that the HMIS Lead Agency will take to implement the plan and monitor progress to meet data quality benchmarks.
- Establish a timeframe for implementing the plan to monitor the quality of data on a regular basis
- In accordance with the HMIS standards outlined by the U.S. Department of Housing and Urban Development, this Privacy plan will be reviewed and updated annually.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Introduction

Bitfocus Inc.

Bitfocus is a consultancy firm that provides the following HMIS Implementation services to the HMIS Lead Agency:

- HMIS Software and Server Administration
- Telephone Help Desk Support
- Ticket Support
- HMIS Implementation and Maintenance
- Remote Web Based and On-Site Training
- Remote Web Based and On-Site Technical Assistance
- Training Manual and Procedural Documentation
- Custom Report Writing
- Data Warehouse Development and Administration
- HMIS Working Group Meeting engagement
- Planning and Policy Making
- AHAR, APR, and QPR support

Bitfocus Inc. provides HMIS Administration services for:

- Northern Nevada Continuum of Care (CoC)
- Southern Nevada Continuum of Care (CoC)
- Balance of State Continuum of Care (CoC)

The Clarity Human Services HMIS Application

The Clarity Human Services HMIS Application is a cloud-based system that offers a comprehensive and end-user adjustable HMIS solution to meet the multiple integration, implementation, and management requirements of the state of Nevada Continuums of Care.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

General Description of HMIS Information Sensitivity

Clarity Human Services HMIS application stores and protects confidential individually identifiable health information. As such, it is equipped with a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

Definition of Data Quality

Data Quality is defined as the reliability and validity of client-level data collected in the HMIS.

General Description of Information Sensitivity

Clarity Human Services HMIS application stores and protects confidential individually identifiable health information. As such it is equipped with a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

Applicable Laws Or Regulations Affecting The System

HMIS Data Standards Revised Notice, U.S. Department of Housing and Urban Development, March 2010

In 2004, HUD published HMIS Data and Technical Standards in the Federal Register. These standards define the requirements for data collection, privacy safeguards, and security controls for all local HMIS. In March 2010, HUD published changes in the HMIS Data Standards Revised Notice incorporating additional data collection

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

requirements for the Homelessness Prevention and Rapid Re-Housing Program (HPRP) funded under the American Recovery and Reinvestment Act (ARRA).

Bitfocus Inc. implements a formal procedure to monitor the ongoing quality of the data entered into the HMIS. All HMIS operations remain in accordance with the most current HMIS Systems requirements as prescribed by HUD.

Data Quality Enforcement

Bitfocus enforces a Data Collection Commitment which states that participation in the HMIS requires that all participating agencies collect minimum data elements on all consenting clients in accordance with HUD requirements

Data Entry Timeliness

Client information, including intake data, program entry dates, services provided, and program exit dates are entered into the HMIS within a reasonable period of time.

To reduce human error that occurs when too much time has elapsed between the data collection (or service transaction) and the data entry, Bitfocus requires participating agencies to specify a reasonable and effective period of time within which data must be entered after interview/intake. These timeframes are dependent upon agency and program type (i.e. g Emergency Shelter, Transitional Housing, Permanent Housing, Safe Haven, Outreach, Prevention, HPRP, or any other programs in the CoC).

Bitfocus participating agencies have designated benchmarks for the following program types:

- **Emergency Shelter programs:** All Universal and Program-Specific Data Elements entered within a specified period of days from intake.
- **Transitional Housing:** All Universal and Program-Specific Data Elements entered within a specified period of days from intake.
- **Permanent Housing:** All Universal and Program-Specific Data Elements entered within a specified period of days from intake.
- **Outreach programs:** Limited data elements entered within a specified period of days from the first outreach encounter. Upon engagement for services, all remaining Universal Data Elements entered within a specified period of days.
- **Prevention programs:** All Universal and Program Specific Data Elements entered within a specified period of days from intake.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Data Completeness & Accuracy

All clients receiving services are entered into the HMIS, and all of the appropriate data elements are collected and entered into the HMIS.

All HMIS data accurately and consistently matches information recorded on paper intake forms and in client files, and HMIS data elements are collected in a consistent manner.

Clarity Human Services HMIS is specifically designed with data quality safeguard programming that requires 100% data completion for all clients entered, for each of the HUD data element sets, as well as bed utilization rates.

This 100% data completion facilitates confident reporting and analysis on the nature and extent of homelessness, such as:

- Unduplicated counts of clients served at the local level;
- Patterns of use of people entering and exiting the homeless assistance system
- Evaluation of the effectiveness of homeless systems

It is vital that CoCs have a HMIS that complies with current HUD required Universal and Program Specific Data Elements. CoCs must also be equipped with a HMIS that can adapt to any future amendments to HUD standards and requirements. This type of preparedness requires a HMIS with highly customizable screens and data fields that can be quickly and seamlessly adapted to meet fluctuating standards and requirements. The Clarity Human Services Screen Designer, Field Editor, and Automated Email Reports equip System Administrators with the capacity to meet and adapt to all HUD requirements and standards.

Clarity Human Services incorporates advanced Data Quality mechanisms. These mechanisms allow automated oversight and seamless ease to correct Data Quality discrepancies based on our Data Quality Model.

Our Data Quality model is built around the following features:

- **Drill-down Reports:** All reports included in our standard report library allow drill-down functionality. For example, when reviewing a report, such as the Annual Performance Report, the value of "Don't Know" may be set to 30. By simply clicking on the number "30" a sub-report will be immediately displayed identifying the clients with incorrect data. The selected clients can be immediately corrected, the APR run again, and the Annual Performance Report will display the updated corrections.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

- **Automated Email Reports:** On a weekly or monthly basis, Our "Emailed Reports" can be automatically sent in PDF form to a recipient list of primary contacts or program managers at each participating agency. These reports provide Data Quality scoring on the Universal Data Elements down to the user/ staff level.

- **Screen Designer tool:** Our screen designer tool can be incorporated to ensure the fields you would like to make 'Required' or 'Soft Required' provide the user with the proper feedback to ensure completion.

In addition, each agency must develop a written program specific interview guide that includes the minimal data elements and any additional elements the agency wishes to collect.

Bed Utilization: Clarity Human Services provides a comprehensive report titled the "Housing Census" Report. This report offers three tiers of drill-down functionality. When the report is processed, the initial parameters request which housing programs to include and the date range of observance. Upon processing of the report, a census of clients is presented for each day of the report. The date itself can then be selected to launch the sub-report detailing all clients represented on that given day. Each client name can then be selected to access the third tier of drill-down, highlighting any poor data quality elements.

These processes are the same across transitional housing and permanent housing, and are also the same for individual beds and units.

Data Quality Monitoring

The Nevada CoCs recognize that the data produced from the Clarity Human Services HMIS is critical to meet the reporting and compliance requirements of individual agencies and the CoC as a whole. As such, all HMIS agencies are expected to meet specified data quality benchmarks. To achieve this, reporting and user feedback is used to quickly identify and resolve issues that affect the timeliness, completeness, and accuracy of the data.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Data Quality Adherence: Incentives and Enforcement

The purpose of monitoring is to ensure that the agreed-upon data quality benchmarks are met to the greatest possible extent and that data quality issues are quickly identified and resolved. To ensure that service providers have continued access to the expectations set forth in the data quality plan, the following protocol will be used:

1. **Access to the Data Quality Plan:** The data quality plan will be available to the general public.
2. **Access to Data Quality Reports:** The HMIS Lead Agency will make data quality reports available for the purposes of facilitating compliance review by participating agencies and the CoC Data Committee.
3. **Data Correction:** Participating agencies will have a specified period of days to correct data. The HMIS Lead Agency will make revised data quality reports available to the general public.
4. **Monthly Review:** The CoC Data Committee will review participating agency data quality reports for compliance with the data quality benchmarks. The Committee will work with participating agencies to identify training needs to improve data quality.
5. **Public Review:** The HMIS Lead Agency will make agency aggregate data quality reports available to the general public.
6. **CoC Review:** The CoC Data Committee will provide a brief update on progress related to the data quality benchmarks at the regularly scheduled CoC meetings.

For agencies that fail to meet the data quality benchmarks, the CoC may ask the agency to submit a written plan that details how they will take corrective action. The plan will be submitted to, and monitored by, the CoC's Data Quality Subcommittee. Should the problem persist, the Data Quality Subcommittee may make a recommendation to suspend the agency's ability to enter data into the HMIS, and will contact any appropriate state and federal funders.

CLARITY
HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT K

HMIS Privacy Plan

>>PLEASE SEE FOLLOWING PAGES<<

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Information Security Department

HMIS PRIVACY PLAN

Purpose: The purposes of this HMIS Privacy Plan are as follows:

- Provide an overview of the privacy requirements of the Clarity Human Services HMIS application, and describe the controls in place or planned for meeting those requirements; and
- Delineate responsibilities and expected behavior of all individuals who access the system.

In accordance with the HMIS standards outlined by the U.S. Department of Housing and Urban Development, this Privacy Plan is to be reviewed and updated annually.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Introduction

Bitfocus Inc.

Bitfocus is a consultancy firm that provides the following HMIS Implementation services to the HMIS Lead Agency:

- HMIS Software and Server Administration
- Telephone Help Desk Support
- Ticket Support
- HMIS Implementation and Maintenance
- Remote Web Based and On-Site Training
- Remote Web Based and On-Site Technical Assistance
- Training Manual and Procedural Documentation
- Custom Report Writing
- Data Warehouse Development and Administration
- HMIS Working Group Meeting engagement
- Planning and Policy Making
- AHAR, APR, and QPR support

Bitfocus Inc. provides HMIS Administration services for:

- Northern Nevada Continuum of Care (CoC)
- Southern Nevada Continuum of Care (CoC)
- Balance of State Continuum of Care (CoC)

The Clarity Human Services HMIS Application

The Clarity Human Services HMIS Application is a cloud-based system that offers a comprehensive and end-user adjustable HMIS solution to meet the multiple integration, implementation, and management requirements of the state of Nevada Continuums of Care.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

General Description of HMIS Information Sensitivity

Clarity Human Services HMIS application stores and protects confidential individually identifiable health information. As such, it is equipped with a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

Applicable Laws Or Regulations Affecting The System

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA's Privacy Rule states that "Individually Identifiable Health Information" is to be considered "protected health information" [PHI] subject to the review and control of individual patients. Agencies and other entities handling PHI are mandated to restrict access to such information to appropriate persons and protect the privacy of individuals. Clarity Human Services includes customization features at micro and macro levels to automate the enforcement of federal, state, and local privacy requirements such as HIPAA.

Clarity Human Services Security Tools enable each partner agency to define which client data is shared with other agencies at every level, including the field level. The default data sharing setup associated with each partner agency can be defined on an agency-by- agency basis (i.e., Agency A may share all client data with Agency B, nothing with Agency C, and only core ID data with Agency D). Our privacy settings can be adjusted to override the default privacy configuration of each agency upon the request of the client.

Bitfocus, Inc. can confirm the capacity of Clarity Human Services to both meet and surpass current HIPAA & HUD requirements and the pending updates to the these requirements.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Participation Requirements

For most efficient utilization of the services provided by the Clarity HMIS, several steps must be completed at the agency level before implementation can begin. Although the Clarity System Administrator can assist with most steps, agencies should be prepared to act without assistance. These steps include:

- Acquisition of High Speed Internet Connectivity with at least one static IP address
- Identification of an on-site Technical Administrator to serve as the primary contact, or the name of an outside contractor.
- Completed network and security assessment to comply with HUD HMIS Data Standard Regulations (4.3 – Security Standards), as published in the July 30, 2004 Federal Register.
- Signed Memorandum of Understanding.

Written procedures concerning client consent for release of information, client grievance procedures and interview protocols

Client Rights and Control

With limited exception, HIPAA vests the control of personal data to patients [e.g. clients]. Each individual patient has the right to review personal data, and to determine who can see these data. Clarity Human Services provides multiple options, including bio-metric technologies, to confirm client identity and to provide options for patients to review their own data. Clarity Human Services also has a Client Forms tool that stores data-sharing consent agreements, and enables authorized users to make client-specific adjustments for overriding general data-sharing settings to meet the specific requests of individual clients

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Documentation of Compliance

While not specified in the statute, organizations dealing with PHI must have the capacity to effectively and efficiently document their compliance with HIPAA. Clarity Human Services has multiple tools and features for documenting HIPAA compliance. A built-in Transaction Log records every change to client data. In addition, there is also an Access Tracking Tool, which displays users who have viewed a client record and when they viewed it. Finally, our reporting tools provide pre-designed and ad-hoc reports for reviewing the access and use of client data

Identity Access Management

Clarity Human Services provides three standard authentication methods to ensure secure authentication, and other identification and access management functions, including:

A. **Basic Authentication** – User must provide login and complex password credentials.

B. **IP Whitelist** – User or Agency must access the system through a pre-approved list of IP Addresses.

C. **Personal PKI Certificate** – User or Agency must have a valid PKI certificate installed within their Browser to access the system. The system administrator can fully administer each method of authentication.

General Operational Controls

Written Client Consent Procedure for Data Entry

Agencies must obtain the client's consent prior to entering information concerning a client into the system. If a client does not consent, services should not be denied to the client. The agency can use the anonymous client function in appropriate cases.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Confidentiality and Consent Forms

Agencies must use the forms approved by the Clarity Working Group. Agencies that share protected health information must have internal procedures for obtaining client consent prior to the sharing of this information.

Privacy Notice

Agencies must develop a privacy notice, and incorporate the Clarity Privacy Notice into its policies and procedures. In addition, HUD mandates that organizations develop policies and procedures to distribute privacy notices to their employees, which include having employees sign to acknowledge receipt of the notices.

Background Check Procedures

Each agency is responsible for conducting its standard background check for all users of the Clarity system.

Staff Confidentiality Agreements

Each agency must develop a procedure for informing staff of client confidentiality. All users of the system must have training prior to being authorized to use the system. In addition, all users of the system are required to attend Clarity confidentiality and privacy training each year.

Information Security Protocols

Internal policies must be developed at each participating agency to establish a process for the detection and prevention of a violation of any HMIS information security protocols.

Virus Prevention, Detection, and Disinfection Protocols

Participation in the HMIS requires that agencies develop procedures intended to assure that computers with access to the HMIS system run updated anti-virus software.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Security Training

User, Administrator and Security Training: Clarity Human Services has provided training to instruct the Clarity System Administrator in the proper procedures to supervise and maintain the operation of the HMIS. System Administration training has covered security, configuration and user customization.

Participating Agency Technical Administrator / Security Officer Training

Each agency participating in the Clarity system will have a Technical Administrator / Security Officer who will be the contact person for participation in the HMIS. Each organization participating in the Clarity system will have a representative participate in the Participating Agency Technical Administrator Training Program prior to system deployment at that agency. Refer to section 2.8 HMIS Software Training for details regarding responsibilities and duties of the Technical Administrator / Security Officer.

Training will take place in Nevada and participants are not to exceed fifteen persons per training. These trainings will cover practical problem solving. Each agency's Technical Administrator will learn how to adjust eligibility screens, identify service data that must be migrated to the HMIS, and how to track expenses and customize the system for his or her organization. Each Participating Agency Technical Administrator will have access to a master manual for program management and will be responsible for either copying or purchasing a copy in house for use at his or her organization. Upon conclusion of the training and prior to deployment, Technical Administrators will begin inputting their HMIS information, number of beds (if any), services, and contact information into the system.

End User Training

Bitfocus will provide training in the day-to-day use of the Clarity system. Training class size will be limited. Training will use an established demo database, and will cover the following topics: intake, assessment, information and referral, reports, and client tracking. Training on any agency-modified fields/screens will be the responsibility of the agency making the modification. Training requires an eight to twelve hour commitment over the course of two days.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

User, Location, Physical and Data Access

Access Privileges to the Clarity System

Access to system resources will only be granted to agency staff that needs access in order to perform their jobs.

Access Levels for Clarity System Users

Each user of the system will be assigned an account that grants access to the specific system resources that he or she requires. A model of least-privilege is used; no user will be granted more than the least amount of privilege needed to perform his or her job.

Access to Data

All data collected by the Clarity system project will be categorized. Access to data sets, types of data, and all other information housed as part of the system is governed by policies approved by the HMIS Working Group and Bitfocus. Reproduction, distribution, destruction of and access to the data are based on the content of the data. At no time may identifying confidential data be distributed or accessible without the consent of the client.

Access to Client Paper Records

Agency users should not have greater access to client information through the Clarity system than is available through the agency's paper files.

Physical Access Control

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

All equipment or media containing HMIS data must be physically controlled at the central site. Protection and destruction of data policies are outlined below. The building containing the central server is secured through locked key access. The room housing the central server has keyed entry with access to keys limited to: Clarity System Administrator, his or her supervisor and the HMIS Project Manager. Access to the central server room is limited to authorized personnel under supervision of the Clarity System Administrator or HMIS Project Manager. All guests will be required to sign in prior to entry. The sign in sheet will be stored and can be produced upon request. All media containing HMIS data will be stored in a fire-protected safe. When necessary, archived media will be destroyed through reformatting and destruction. All hard drive media, optical media and magnetic floppy media taken out of service will be disassembled and the platters physically destroyed.

System access over wired networks

Access to the HMIS system over any type of wireless network is discouraged. Wireless networks are more susceptible to unauthorized access than wired networks. If any type of wireless network is used, it must have at least 128-bit encryption. If 128-bit encryption is not available, each client workstation must have VPN client software installed.

Unique User ID and Password

Each user of the system must be individually and uniquely identified. Identification will be verified through a password. Users are not permitted to share their password or permit other users to log in to the system with their password. Passwords will be at least eight characters long and meet reasonable industry standard requirements. These requirements are:

3. Using a combination of at least 3 of the following:
    - Numbers
    - Lowercase letters
    - Capital letters
    - Special characters (e.g. ~ ! @ # $ % ^ & * ( ) _)
4. Not using, or including, the username, the HMIS name, or the HMIS vendor's name
5. Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users will not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

Right to Deny User and Participating Agencies' Access

The Working Group has the right to suspend, limit or revoke the access of any agency or individual for violation of HMIS policies. Upon remedy of said violation, access rights may be reinstated. If privileges have not been reinstated, the person or agency can file an appeal to the HMIS Working Group for reinstatement.

Monitoring

Access to the system will be monitored. In addition, the Clarity system will maintain logs of all actions taken within the system including login transactions and detailed monitoring of user data transactions within the software. Bitfocus will use its best reasonable efforts to review logs on a regular basis. It is understood that agencies will cooperate with all monitoring requirements. All exceptions that show security policy violations will be investigated.

Data Integrity Controls

Access to the production data is restricted to essential system administrative staff only. Each staff that has access to production data is contracted to not alter or impact the data in any adverse way.

Data Release Protocols

Data Entry

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Before any data will be entered into the system, the client must first consent to data entry and agree to what information can be entered into the Clarity system. Upon completion of the approved consent form, the service provider will only enter the information into the system that has been approved by the client. The Clarity system will assign the client a unique personal identifier. Service providers should note that services must not be contingent on a client consenting to data entry.

Anonymous Client Data Entry

In the event that a client does not want to have any of their information entered into HMIS, they will be entered as a "John/Jane Doe" and all of the information entered into the system fields will be zeros. The HMIS will assign them a unique personal identifier.

Sharing of Information

Clients must consent to the sharing of their information prior to allowing that information to be shared with participating agencies. In the event that the client agrees to have their information entered into the HMIS but does not agree to have it shared with other agencies, selecting the "Local Only" option available in the Clarity system will close the entire record.

Sharing of Protected Information

A separate Release of Information (ROI) indicating what information the client agrees to have shared with other participating agencies should be signed prior to sharing of any Protected Personal Information (PPI).

Printed Information

Printed records disclosed to the client or another party should indicate: the person and/or agency to whom the record is directed, the date, and the initials of the person making the disclosure.

Requests for HMIS Client Information

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

The agency must notify the HMIS Program Administrator within one working day when the agency receives a request from any individual or outside organization for client-identifying information.

Case Notes

It is understood that client case notes will not be shared, and that each agency will have the ability to enter its own private notes about a client.

The Release of Information (ROI) form will be a dated document that expires. The provider will only be able to access the information specified on the ROI that was entered into the system during the time the ROI was in effect. Also, the client can decide at any time that he or she wants to have their information closed, in full or in part, and/or client file deactivated.

Internal Operating Procedure

Computer Virus Prevention, Detection, and Disinfection

The Clarity system will be to incorporate and maintain updated virus protection from a reputable single source. Any and all viruses found will be quarantined and analyzed. If unrepairable, the virus will be deleted. Participating agencies are required to run and maintain their own anti-virus software from an approved source on all computers that have access to the HMIS system.

Operating System Updates

The HMIS system will be updated and patched within a reasonable time after review of the vendor's release of updates and patches and approval by the system administrator.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Backup and Recovery

Backup will occur on a regular basis Backup media will be stored in a fire-protected safe with the server. In addition, backups will be stored electronically, offsite. A backup of hardware and Clarity system software will be stored in an offsite location so that it will be available in the event of catastrophic failure.

Disaster Recovery Process

Disaster recovery processes will be reviewed as prescribed by HUD, and offsite and offsite systems will be checked for viability twice per year.

Community Reporting Process

At the direction of the Working Group, Bitfocus will publish community-wide aggregate reports on the clients in the HMIS system on a periodic basis. These report(s) will reflect raw, point-in-time data.

Termination of the HMIS system

In the event the Clarity HMIS ceases to exist, participating agencies will be notified and provided a reasonable time to access and save client data on those served by the respective agencies as well as statistical and frequency data from the entire system. Then, the information on the central server will be purged or stored. If the latter occurs, the data will remain in an encrypted and aggregate state.

Termination of Bitfocus as Program Administrator

In the event Bitfocus is no longer the program administrator, custodianship of the data on the HMIS system will be transferred to the HMIS Working Group or to a successor program administrator, and all participating agencies will be informed in a timely manner.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

HMIS Privacy Notice

An individual has a right to adequate notice of the uses and disclosures of protected personal information that may be made by a participating agency and of the individual's rights and the participating agency's legal duties with respect to protected personal information. The notice should be prominently displayed in the program offices where intake occurs. The participating agency should promptly revise and redistribute its notice whenever there is a material substantive change to the permitted uses or disclosures, the individual's rights, the Participating Agency's legal duties, or other privacy practices stated in the notice. Participating agencies should maintain documentation of compliance with the notice requirements by retaining copies of the notices issued by them. A client has the right to obtain a paper copy of the notice from the participating agency upon request. An inmate does not have a right to notice, and the requirements of this notice do not apply to a correctional institution that is a Clarity system user.

Content of Notice: *The Participating Agency must provide a notice that is written in plain language and that contains the elements required by this section. These elements are not exclusive, and either oral or written notice may inform the individual of the permitted uses of information. The following statement as a header or otherwise must be prominently displayed: "THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."*

A description of each of the purposes for which a participating agency is permitted or required by this notice to use or disclose protected personal information without the individual's written consent or authorization. These include administrative, programmatic, and academic research purposes.

If a use or disclosure is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

A statement that consensual uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization.

A statement of the individual's rights with respect to protected personal information and a brief description of how the individual may exercise these rights.

A statement that the participating agency is required by law to maintain the privacy of protected personal information and to provide individuals with notice of its legal duties and privacy practices with respect to protected personal information.

A statement that the participating agency is required to comply with the terms of the notice currently in effect.

A statement that reserves the right to change the terms of the notice and to make the new notice provisions effective for all protected personal information. The statement must also describe how the agency will attempt to provide individuals with a revised notice.

A statement that individuals may complain to the participating agency if they believe their privacy rights have been violated.

A brief description of how the individual may file a complaint with the participating agency.

A statement that the individual will not be retaliated against for filing a complaint.

The name, or title, and telephone number of a person or office to contact for further information.

The date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Guidelines on Removing Agencies or Users

Voluntary Removal

If an agency or user no longer wants to access the Clarity system, they simply need to contact Bitfocus and inform them of the decision. In the case of user removal, it is the relevant agency's responsibility to contact Bitfocus in a timely fashion so the User ID can be deactivated to prevent unauthorized access to the system. An agency asking to be removed from the system understands the following:

1. The agency will receive one (1) copy of the data it has input into the Clarity system. This copy will be in a format determined by Bitfocus and approved by the Working Group. The agency will be given an appropriate description of the data format.
2. The data the agency enters into the system will remain in the system for the purposes of producing aggregate non-identifying reports. Client records will be marked as inactive, and not be available to be accessed. Any agency information will remain in the system, but will be marked as inactive.
3. The agency must return all hardware (firewalls, etc.) that are owned by Bitfocus.
4. Any fees paid for participation in the Clarity HMIS system will not be refunded.
5. The agency understands and accepts any ramifications for not participating in the Clarity system.

Involuntary Removal

It is vital for the Working Group and Bitfocus to provide a secure service for all users. Any action(s) that threaten the integrity of the system will not be tolerated.

1. Bitfocus reserves the right to modify, limit and/or suspend any user account at any time if there is a security risk to the system
2. Any improper use of the Clarity System is subject to immediate suspension of the user's account. The penalties imposed on a user for improper system use will vary based on the level of the offense. Typically the user will receive a warning on the first offense. However, if the offense is severe enough, Bitfocus reserves the right to disable the account immediately and in extreme cases, may disable all users' access by the agency in question.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

3. Bitfocus will contact the organization within one business day of any suspension.
4. If a users account is suspended, only the director (or acting director) for an organization may request account re-activation. Suspended users may be required to attend additional training before having their access reinstated.
5. In the event that an agency is removed from the system they must submit a written request for reinstatement to the Working Group and Bitfocus. If an agency is not reinstated into the system after review, the agency will be given one (1) copy of its data in a format that will be determined by Bitfocus and approved by the Working Group (the agency will also be provided with a description of the data format). Data will not be given to the agency until all hardware (firewalls, etc.) belonging to Bitfocus is returned. Any fees paid for participation in the Clarity system will not be returned.
6. All Clarity system users agree to waive and release any and all claims and expenses related to or arising from the user's violation of this agreement against the Working Group, the employers of the respective members of the Working Group, Bitfocus, its officers, directors, shareholders, employees, agents, subsidiaries and affiliates.

Participation Security Standards

System/Data Security

In the event an agency becomes aware of a system security or client confidentiality breach, the executive director of the agency shall notify the HMIS Program Administrator of the breach within one business day.

HMIS Related Forms and Printed Material

Any HMIS forms or printed information obtained by an agency or user from the HMIS system must be destroyed in a manner that ensures client confidentiality will not be compromised.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

HMIS CONCEPTS & TERMS

Aggregate - Collected together from different sources and considered as a whole, and lacking identifying information.

Client - Somebody who uses or applies to use the services of a participating agency.

CoC – The acronym for Continuum of Care

Community - A group of people with a common background or with shared interests within a defined geographic area, for our area to include the state of Nevada.

Confidentiality - Entrusted with somebody's personal or private information or matters.

Connectivity – The ability to connect two or more systems together. Pertaining to the HMIS system, the use of a high speed Internet connection for accessing the system.

Consent – Express acceptance of or agreement to something.

Data – The information in the system, for example, numbers, text, images, and sounds, in a form that is suitable for storage in or processing by a computer

Decryption – To render an encoded amount of data into plain language or out of its encrypted state.

Encryption – To convert computer data and messages to something incomprehensible by means of a key, so that only an authorized recipient holding the matching key can reconvert it.

Firewall – A component of a network that prevents unauthorized users and/or data from getting in or out of the network, using rules to specify acceptable communication

HMIS – The acronym for Homeless Management Information Systems, sometimes also referred to as HIMS or Homeless Information Management System.

HUD – The acronym for the Department of Housing and Urban Development.

Legacy Data – Information stored in an older version of software or format that is not compatible with the HMIS system.

Clarity Human Services– The name of the software application that being used for the Clarity HMIS.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

Clarity System – The name that has been given to our implementation of an HMIS system.

MOU – The acronym for Memorandum of Understanding. A document that outlines the specific areas of agreement between two or more parties.

Organization - A group of people identified by shared interests or purpose.

PPI – The acronym for Protected Personal Information.

Program – A collection of services grouped together.

ROI – The acronym for Release of Information.

Service - The system or operation by which people are provided with something.

VPN – The acronym for Virtual Private Network. A way for securely connecting systems together to transmit data.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

EXHIBIT L

Nevada Statewide HMIS Working Group

Memorandum of Understanding

With

{Enter CoC Name}

This agreement has been made and entered into between the Nevada HMIS Working Group and the {Enter CoC Name} Continuum of Care and is to be reviewed for possible modification and/or reassignment one year from today, {Enter Current Date}.

Mutual Understanding

The Nevada HMIS Working Group and the {Enter CoC Name} Continuum of Care, hereinafter referred to as the CoC, agree to collaboratively manage the implementation, administration, and maintenance of the Homeless Management Information System (HMIS) database for Nevada.

The purpose of the Nevada HMIS Working Group is to ensure the set up and implementation of the HMIS database meets the combined needs of all homeless service providers throughout the state. Furthermore, the Nevada HMIS Working Group plans for and monitors consistent data entry and accurate reporting on the statewide level and provides a supportive network for HMIS staff within each participating Continua of Care.

Roles and Responsibilities: Nevada HMIS Working Group

The Nevada HMIS Working Group is responsible for providing counsel and assistance to the staff members, governing bodies, and contributing providers within each of the four participating continua of care on all matters HMIS. The responsibilities of the Nevada HMIS Working Group include but are not limited to the following:

1. Participate in system-level HMIS implementation decision making that accommodates the needs and concerns of each Continuum of Care.
2. Develop and maintain policies and procedures designed to ensure consistent and effective use of the statewide HMIS database and software system.
3. Collaborate and support statewide HMIS operations to include coordinated training, addition of state and federal partners, technical enhancements, module expansion, and other activities as defined by the Nevada HMIS Working Group.

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

4. Disseminate information about the statewide HMIS database, the steering committee and its activities, policies, and procedures.
5. Provide counsel and assistance to HMIS staff within each participating continua of care.
6. Identify, develop, and implement strategies for improving HMIS coverage and data quality throughout Nevada.
7. Establish security and privacy policies at the statewide level.
8. Identify and diminish potential barriers to the use and improvement of the statewide HMIS database.
9. Adhere to the code of conduct as set forth in the By-Laws of the Nevada HMIS Working Group.
10. Recognize that the Nevada HMIS Working Group has no authority to recommend the termination of, dissolve, or discredit any continua's programs or activities or govern the continua.
11. Upon request for statewide-level reports, the Nevada HMIS Working Group will review the report, agree upon the contained data, and/or provide contextual explanation and clarification prior to distribution to requester. If a CoC feels the data for their CoC is not adequately representative, the CoC may choose to have their data removed from the statewide report. Additionally, the Nevada HMIS Working Group cannot use HMIS data to make blanket statements about the effectiveness of programs statewide.

Roles and Responsibilities: {Enter CoC Name}

The {Enter CoC Name} remains responsible for the daily functioning of HMIS within the CoC's geographic region while supporting and adhering to the decisions, policies, and procedures established by the Nevada HMIS Working Group. To this effort, the responsibilities of the CoC include but are not limited to the following:

1. Designate two representatives to serve on the Nevada HMIS Working Group. These representatives shall include a representative with decision-making capacity from the HMIS Lead Agency as well as HMIS staff. If necessary, the CoC may choose to designate a non-HMIS staff member with decision-making capacity for HMIS purposes.
2. Continue to secure funding for the HMIS project at the CoC level from federal, local and/or private funding source. Per HUD guidance, the individual CoC is not required to merge the HMIS grant into a statewide HMIS grant. Each continuum deserves the right to prioritize its own programs and determine how to resolve homelessness.
3. Enter into and manage HMIS Participation Agreements between the HMIS Lead Agency and Contributing HMIS Organizations (CHOs) within the CoC.
4. Reviewing and evaluating HMIS reports for the CoC and the programs within its geographic jurisdiction.
5. Identify, develop, and implement strategies for improving HMIS coverage and data quality within the CoC's geographic jurisdiction.
6. Collecting, storing, and updating program descriptor data element information about each Contributing HMIS Organization within the CoC.
7. Communicating with CHOs, stakeholders, government officials, and the CoC governing body regarding all matters HMIS.
8. Provide training and technical assistance for the HMIS users within the CoC. Training is provided by the HMIS System Administrator, Bitfocus, Inc.
9. Monitoring adherence to the statewide security and privacy policies at the CoC level.
10. Coordinating HMIS-related issues as agenda items for the appropriate CoC meetings.

CLARITY HUMAN SERVICES

T: 702.605.6870
F 702.666.9102
TF 888.866.1533
E nevada@bitfocus.com

_____ _____

Chair, Nevada HMIS Working Group Date

_____ _____

CoC Board Chair, {Enter CoC Name} Date

Opt Out: {Enter CoC Name}

ONLY complete this section if the CoC has decided to NOT participate with the Statewide HMIS Working Group governance model.

Effective {Enter Date}, the {Enter CoC Name} CoC no longer agrees to be accountable for the roles and responsibilities outlined in this document.

_____ _____

CoC Board Chair, {Enter CoC Name} Date