The following is an excerpt from the HMIS Policy and Procedure Manual

3.1 BASELINE PRIVACY POLICY

Upon request, clients must be able to access the *Baseline Privacy Policy* found below

Collection of Personal Information

Personal information will be collected for the Homeless Management Information System (HMIS) only when it is needed to provide services, when it is needed for another specific purpose of the agency where a client is receiving services, or when it is required by law. Personal information may be collected for these purposes:

- To provide or coordinate services for clients
- To find programs that may provide additional client assistance
- To comply with government and grant reporting obligations
- To assess the state of homelessness in the community, and to assess the condition and availability of affordable housing to better target services and resources

Personal information must be collected with the knowledge and consent of clients. It is assumed that clients consent to the collection of their personal information as described in this notice when they seek assistance from an agency using HMIS and provide the agency with their personal information.

Personal information may also be collected from:

- Additional individuals seeking services with a client
- Other private organizations that provide services and participate in HMIS

Use and Disclosure of Personal Information

These policies outline how personal information may be used and disclosed by the Institute for Community Alliances (ICA) on behalf of the four Wisconsin Continua of Care, subject to oversight by the Wisconsin HMIS Advisory Board. Participating organizations may have separate privacy policies and that may allow different uses and disclosures of personal information. If clients access services at one of these organizations, they can request to view that agency's privacy and sharing policy.

The primary reason why personal information may be used or disclosed is to provide or coordinate services to individuals. To accomplish this goal, client data may be shared among HMIS-participating providers as well as with non-participating network partners—that is, agencies with which ICA has a written data sharing agreement. Through the HMIS Agency Agreement and ICA data sharing agreements, ICA will ensure that client data is used and disclosed only for purposes that improve service delivery for individuals.

Agencies collecting client information are required to notify clients that their personal information may be shared through the posting of the HMIS Consumer Notice.

Personal information will be used or disclosed without written client consent for activities described below. Clients must give consent before their personal information is used or disclosed for any purpose not described here:

1. To carry out administrative functions such as legal audits, personnel, oversight, and management functions.

2. For academic research, program analysis or statistical purposes conducted by an individual, organization or institution that has a formal relationship with the Institute for Community Alliances. The research must be conducted by an individual employed by or affiliated with the organization or institution. All research projects must be conducted under a written research agreement approved in writing by the Designated Agency HMIS Contact or executive director. The written research agreement must:
    - Establish the rules and limitations for processing personal information and providing security for personal information in the course of the research.
    - Provide for the return or proper disposal of all personal information at the conclusion of the research.
    - Restrict additional use or disclosure of personal information, except where required by law.
    - Require that the recipient of the personal information formally agree to comply with all terms and conditions of the written research agreement, and
    - Be substituted, when appropriate, by Institutional Review Board, Privacy Board or other applicable human subjects' protection institution approval.

3. When required by law. Personal information will be released to the extent that use or disclosure complies with the requirements of the law.

4. To avert a serious threat to health or safety if:
    - the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
    - the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

5. To report to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence, information about an individual reasonably believed to be a victim of abuse, neglect or domestic violence. When the personal information of a victim of abuse, neglect or domestic violence is disclosed, the individual whose information has been released will promptly be informed, except if:
    - it is believed that informing the individual would place the individual at risk of serious harm, or
    - a personal representative (such as a family member or friend) who is responsible for the abuse, neglect or other injury is the individual who would be informed, and it is believed that informing the personal representative would not be in the best interest of the individual as determined in the exercise of professional judgment.

6. For a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
    - In response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer or a grand jury subpoena, if the court ordered disclosure goes through the Institute for Community Alliances and is reviewed by the Executive Director for any additional action or comment.

- If the law enforcement official makes a written request for personal information. The written request must meet the following requirements:
    i. Be signed by a supervisory official of the law enforcement agency seeking the personal information.
    ii. State how the information is relevant and material to a legitimate law enforcement investigation.
    iii. Identify the personal information sought.
    iv. Be specific and limited in scope to the purpose for which the information is sought, and
    v. Be approved for release by the Institute for Community Alliances legal counsel after a review period of seven to fourteen days.
- If it is believed that the personal information constitutes evidence of criminal conduct that occurred at the agency where the client receives services.
- If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to a foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

7. For law enforcement or another public official authorized to receive a client's personal information to conduct an immediate enforcement activity that depends upon the disclosure. Personal information may be disclosed when a client is incapacitated and unable to agree to the disclosure if waiting until the individual is able to agree to the disclosure would materially and adversely affect the enforcement activity. In this case, the disclosure will only be made if it is not intended to be used against the individual.

8. To comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

9. In the event of a public health emergency, personal information, including protected health information, may be disclosed to appropriate public health entities to support coordination measures to protect public health.

<u>Inspection and Correction of Personal Information</u>
Clients may inspect and receive a copy of their person information maintained in HMIS. The agency where the client receives services will offer to explain any information that a client may not understand.

If the information listed in HMIS is believed to be inaccurate or incomplete, a client may submit a verbal or written request to have his/her information corrected. Inaccurate or incomplete data may be deleted or marked as inaccurate or incomplete and supplemented with additional information.

A request to inspect or copy one's personal information may be denied if:
- The information was compiled in reasonable anticipation of litigation or comparable proceedings

- The information was obtained under a promise or confidentiality and if the disclosure would reveal the source of the information, or
- The life or physical safety of any individual would be reasonably endangered by disclosure of the personal information.

If a request for inspection access or personal information correction is denied, the agency where the client receives services will explain the reason for the denial. The client's request and the reason for the denial will be included in the client's record.

Requests for inspection access or personal information correction may be denied if they are made in a repeated and/or harassing manner.

Limits on Collection of Personal Information
Only personal information relevant for the purpose(s) for which it will be used will be collected. Personal information must be accurate and complete.

Client files not used in seven years may be made inactive in HMIS. ICA will check with agencies before making client files inactive. Personal information may be retained for a longer period if required by statute, regulation, contract, or another obligation.

Limits on Partner Agency Use of HMIS Client Information
The Wisconsin HMIS is a shared data system. This system allows Partner Agencies to share client information to coordinate services for clients. However, Partner Agencies may not limit client service or refuse to provide service in a way that discriminates against clients based on information the Partner Agency obtained from HMIS. Partner Agencies may not penalize a client based on historical data contained in HMIS.

Youth providers serving clients under the age of 18 must maintain HMIS client files that are not shared. Youth under the age of 18 may not provide either written or verbal consent to the release of their personally identifying information in HMIS.

Complaints and Accountability
Questions or complaints about the privacy and security policies and practices may be submitted to the agency where the client receives services. Complaints specific to HMIS should be submitted to the Designated Agency HMIS Contact and program director. If no resolution can be found, the complaint will be forwarded to the System Administrators, and the agency's executive director. If there is no resolution, the Wisconsin HMIS Advisory Board will oversee final arbitration. All other complaints will follow the agency's grievance procedure as outlined in the agency's handbook.

All HMIS users (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Users must receive and acknowledge receipt of a copy of this privacy notice.

3.2 HMIS INTERNAL PRIVACY SETTINGS

The Wisconsin HMIS is a shared system. The default privacy settings for all client data entered by Partner Agencies are shared. Shared data is unrestricted information that has been entered by one provider and is visible to other providers using HMIS.

All Partner Agencies have the option to change their HMIS project settings to not share their client data with other Partner Agencies. Information entered by one Partner Agency that is not shared will not be visible to other Partner Agencies using HMIS. Projects that provide legal services, or serve individuals with HIV/AIDS, unaccompanied minors, or victims of domestic violence (when the participating agency is not a victim service provider), must have their client data visibility set to not shared. Projects that provide legal services may enter clients as "unnamed." Through the HMIS Release of Information, clients may request that their individual client record is not shared going forward. Client records that were shared and contain data entered by multiple agencies cannot retroactively be closed. Individual components of the client record may be closed but the entire client record cannot be closed.

3.3 PARTNER AGENCY WORKPLACE REQUIREMENTS

1. The agency must apply system security provisions to all the systems where HMIS data is accessed including networks, desktops, laptops, smart devices, mainframes, and servers.
2. When HMIS is accessed in public areas the agency must ensure that the workstation is always supervised by authorized HMIS users. Screens displaying the HMIS may not be visible by unauthorized individuals.
3. Devices and data must be secured when workstations are not in use and staff are not present. Workstations must automatically turn on a password protected screen saver when the workstation is temporarily not in use. Staff are required to log off the HMIS when not at the workstation.
4. The agency must ensure all privacy and security requirements are always adhered to in remote work locations.

3.4 DATA REPORTING PARAMETERS AND GUIDELINES

Upon any request for HMIS System Data, ICA staff will adhere to the following principles for release of data:

- Only de-identified aggregated data will be released except as specified in the HMIS Baseline Privacy Notice.
- Program specific information used for annual grant program reports and program specific information included in grant applications is classified as public information. No other program specific information will be released without written consent.
- There will be full access to aggregate data included in published reports.
- Reports of aggregate data may be made directly available to the public.
- The parameters of the aggregated data, that is, where the data comes from and what it includes will be presented with each report.
- Data will be mined for agencies requesting reports on a case-by-case basis.
- Requests must be written with a description of specific data to be included and for what duration of time. Requests are to be submitted at least 30 days prior to the date the report is needed. Exceptions to the 30-day notice may be made.
- ICA reserves the right to deny any request for aggregated data. Final decisions will be made by the HMIS Director.

3.5 RELEASE OF DATA FOR GRANT FUNDERS

Entities providing funding to agencies or programs required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by ICA when there is a voluntary written agreement in place between the funding entity and the agency or program. Funding for any agency or program using HMIS cannot be contingent upon establishing a voluntary written agreement allowing the funder HMIS access.

3.6 DATA SHARING EXTERNAL TO HMIS

Disclosure of client personal information to third parties requires a formal written agreement, authorized by the HMIS Advisory Board. If an agreement is compatible with a prior authorization that is still in effect, ICA may enter into an agreement that does not require secondary authorization after notifying the HMIS Advisory Board.

Third parties seeking client personal information from the Wisconsin HMIS will be required to complete a standard application designed to gather information regarding the information requested, the rationale for disclosure of the data (i.e., the benefits to persons experiencing/at risk of homelessness), and the scope of the project (i.e. one-time or ongoing). The application will be subject to legal review, after which the HMIS Advisory Board will vote on whether to enter into the proposed agreement.

Third parties with which ICA has a written data sharing agreement for the purpose of service delivery coordination and improvement are referred as “network partners.” As with HMIS-participating agencies, clients will have the opportunity to opt-out of sharing their data with network partners through the HMIS Release of Information. An up-to-date list of network partners will be posted on the ICA Wisconsin website.

Any external sharing of client personally identifiable information will be utilize secure transmission methods that meet industry standards, such as Secure File Transfer Protocol (SFTP), or through the use of an Application Programming Interface (API).

3.7 DATA CATEGORIZATION AND HANDLING

Proper data handling protocols depend on the nature of the information being transmitted or stored:

- Open Data: This is data that contains de-identified, client-level information. The data should be handled discretely, be stored out of sight, and may be transmitted via internal or first-class mail.

- Confidential Data: Confidential data contains personal identifying information, such as name, date of birth, and social security number. Whenever confidential data is accessed:
    - Hard copies shall be shredded when disposal is appropriate. Hard copies shall be stored in a secure environment that is inaccessible to the general public or staff not requiring access.
    - Hard copies shall not be left out in the open or unattended.
    - Electronic copies shall be stored only where the employee can access the data.

    - Electronic copies shall be stored where a password is required to access the data if on shared server space.
    - Electronic copies shall be magnetically overwritten when disposal is appropriate.
    - Encryption required for electronic transmission.

- Aggregated Public Data: Data that is published and available publicly. This type of data does not identify clients listed in the HMIS. Security controls are not required.

- Unpublished Restricted Access Data: Information scheduled, but not yet approved, for publication.
    - Examples include draft reports, fragments of data sets, and data without context or data that have not been analyzed.
    - Accessible only to authorized HMIS staff and agency personnel.
    - Requires auditing of access and must be stored in a secure out-of-sight location.
    - Data can be transmitted via e-mail, internal departmental or first-class mail. If mailed, data must be labeled confidential.

Partner Agency Record Retention Policy
Partner agencies must have a written record retention policy that includes how printed HMIS records are destroyed.

3.8 SECURITY PROCEDURE TRAINING FOR USERS

All users must receive security training prior to being given access to HMIS. Security training will be covered during the new user training for all new users. All users must receive ongoing annual training on security procedures from the Institute for Community Alliances.

3.9 VIOLATION OF SECURITY PROCEDURES

All potential violations of any security protocols will be investigated, and any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to a formal letter of reprimand, suspension of system privileges, revocation of system privileges and criminal prosecution.

If possible, all confirmed security violations will be communicated in writing to the affected client within 14 days, unless the client cannot be located. If the client cannot be located, a written description of the violation and efforts to locate the client will be prepared by the System Administrator at the Institute for Community Alliances and placed in the client's file at the Agency that originated the client's record.

Any agency that is found to have consistently and/or flagrantly violated security procedures may have their access privileges suspended or revoked. All sanctions are imposed by the ICA HMIS staff. All sanctions may be appealed to the HMIS Advisory Board.

3.10 PROCEDURE FOR REPORTING SECURITY INCIDENTS

Users and Designated Agency HMIS Contacts should report all unlawful access of HMIS and unlawful attempted access of HMIS. This includes theft of usernames and passwords. Security incidents should be reported to the ICA System Administrator. The ICA System Administrator will use the HMIS user audit trail report to determine the extent of the breach of security.

3.11 DISASTER RECOVERY PLAN

Bitfocus Disaster Recovery Plan

Wisconsin's HMIS is covered under Bitfocus' Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. The disaster recovery plan is meant to minimize any effects of service outages and to enable Bitfocus to either maintain, or quickly resume, mission-critical functions. A copy of this plan is available for review by submitting a request to the WI HMIS Help Desk.

Standard Data Recovery

Wisconsin's HMIS database is stored online and is readily accessible for approximately 24 hours a day. Tape backups of the database are kept for approximately one month. Upon recognition of a system failure, HMIS can be copied to a standby server. The database can be restored, and the site recreated within three to four hours if online backups are accessible. As a rule, a tape restoration can be made within six to eight hours. On-site backups are made once daily. A restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.

All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that are connected in turn to electrical circuits, which are connected to a building generator.

All client data is backed-up online and stored on a central file server repository for 24 hours. Each night a tape backup is made of the client database and secured in a bank vault.

Historical data can be restored from tape as long as the data requested is newer than 30 days old. As a rule, the data can be restored to a standby server within four hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.

For power outage, HMIS is backed up via APC battery back-up units, which are connected via generator-backed up electrical circuits. For a system crash, a system restore will take four hours. There is potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a tape restore is necessary. If the failure is not hard drive related, the data restore time will possibly be shorter as the drives themselves can be repopulated into a standby server.

All major outages are immediately brought to the attention of executive management. WellSky support staff helps manage communication or messaging to the System Administrator as progress is made to address the service outage.

Wisconsin HMIS Disaster Recovery Plan

The Institute for Community Alliances operates a regional approach to administering the Wisconsin HMIS. The main ICA Wisconsin HMIS office is in Madison, Wisconsin, and there are three regional offices throughout the state. In the event of a localized emergency or disaster, ICA will shift responsibility for administering the HMIS and managing day-to-day operations of the system to an unaffected site.