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

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.
    -

- 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

- 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 receiv

Requests for inspection access or personal information correction may be denied if they are made in a repeated

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

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 (

o

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

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

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 6.66 237.62 -7(A)4(s)-4(a)13( )-48[e2>BD5hima)11(r)( )-4(A)4()14(t)-4(a441.0 Gve k)8(ep)3(

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.