

Big Bend Continuum of Care Homeless Management Information System (HMIS) Privacy Statement

Brief Summary

Updated April 17, 2015

Version 3.0

This notice describes the privacy policies of the Big Bend Continuum of Care (CoC) regarding clients' protected personal information that is collected and resides in the Homeless Management Information System (HMIS) database for the CoC. This notice may be amended only after the proposed change has been recommended by the HMIS/Data/Performance Committee to the full CoC Board and is approved in accordance with the CoC Governance Charter, and the HMIS Governance Charter unless we are required by law to make an immediate change.

Upon appropriate client permission, personal information is collected through the HMIS and Coordinated Intake and Assessment to be used for the following purposes:

- a. To provide or coordinate services to clients;
- b. To locate other programs that may be able to assist clients;
- c. For functions related to payment or reimbursement from others for services that are provided;
- d. To operate as the HMIS lead agency, including administrative functions such as legal, audits, personnel, oversight, and management functions;
- e. To comply with government reporting obligations; and
- f. When required by law.

The Data Privacy Notice & Consent Form is explained to each client. Clients should indicate consent for collecting information for the purposes listed above and detailed within the privacy policy unless otherwise noted. Any individual can inspect his/her personal information in the HMIS. All efforts will be made to correct inaccurate or incomplete information. The privacy policy and/or practices are available for any individual to review at any time. Any questions and/or complaints will be addressed by the HMIS/Data/Performance Committee in a timely manner. Please read the full notice for more details. Any individual may have a copy of the full notice upon request.

Big Bend Continuum of Care HMIS Privacy Statement

Full Notice

Updated March 9, 2015

Version 3.0

A. Privacy Policy & Practices

1. This notice describes the privacy policy and practices of the CoC regarding clients protected personal information that resides in the HMIS database for the eight-county (Franklin, Gadsden, Jefferson, Leon, Liberty, Madison, Taylor, and Wakulla) Big Bend region. The HMIS participating agencies are listed in Appendix A of this document. The Big Bend Homeless Coalition serves as the HMIS Lead Agency for the CoC. The HMIS Lead Agency is located at 325 John Knox Rd, Building B in Tallahassee, FL 32303.
The policy and practices in this notice cover the processing of protected personal information for clients of the CoC and the agencies participating in the HMIS.
2. Protected personal information is any information maintained in the HMIS about a client that:
 - a. Allows for the identification of an individual directly or indirectly;
 - b. Can be manipulated by a reasonable foreseeable method to identify a specific individual; or
 - c. Can be linked with other available information to identify a specific client.
3. This policy was established because of standards for HMIS issued by the Department of Housing and Urban Development (HUD). These policies and practices are to be consistent with those standards (see 69 Federal Register 45888).
4. This notice informs clients, staff, and others how protected personal information is processed. This notice may be amended only after the proposed change has been recommended by the HMIS/Data/Performance Committee to the full CoC Board and is approved in accordance with the CoC Governance Charter and the HMIS Governance Charter unless we are required by law to make an immediate change.
A copy of this privacy notice will be made available to any interested parties.

B. Collection of Personal Information

1. Upon appropriate client permission, personal information is collected only when appropriate to provide services or for another specific purpose of the HMIS Lead Agency or when required by law. Information may be collected for the following purposes:
 - a. To provide or coordinate services to clients;
 - b. To locate other programs that may be able to assist clients ;
 - c. For functions related to payment or reimbursement from others for services that are provided;
 - d. To operate the HMIS Lead Agency, including administrative functions such as addressing legal issues, audits, personnel, oversight, and management functions; and
 - e. To comply with government reporting obligations, when required by law.
2. The HMIS Lead Agency only collects personal information using lawful and fair practices of the highest integrity.

3. HMIS Participating Agencies only collect personal information with the knowledge and consent of the clients. Each client has the right to share their information or choose to not share by signing a Release of Information specific to HMIS. The choice to decline sharing information does not prevent a client from receiving services.

C. Use & Disclosure of Personal Information

1. Any disclosure of personal information through HMIS is available through a shared Coordinated Intake and Assessment process. The sharing of Data and/or Personal Protected Information is part of the open system of care designed to provide the most efficient and effective case management practices for individuals participating in the HMIS. Data and/or Personal Protected Information are not shared if a client requests anonymity.
 - a. To provide or coordinate services to individuals;
 - b. For functions related to payment or reimbursement of services;
 - c. To complete administrative functions such as legal, audits, personnel, oversight, and/or management functions;
 - d. To create de-identified (anonymous) information that can be used for research and statistical purposes without identifying clients;
 - e. When required by law to the extent that use or disclosure complies with and is limited to the requirements of the law;
 - f. To avert a serious threat to health or safety if
 - 1) It is believed that 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
 - 2) The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
 - g. To report an individual reasonably believed to be a victim of abuse, neglect, or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect, or domestic violence
 - 1) Under any of the following circumstances:
 - a) Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
 - b) If the individual agrees to the disclosure; or
 - c) To the extent the disclosure is expressly authorized by statute or regulation; and
 - i. It is believed the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
 - ii. If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the personal information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

and

- 2) When a permitted disclosure about a victim of abuse, neglect, or domestic violence is made, the individual who is the victim will be promptly informed that a disclosure has been made, except if:
 - a) In the exercise of professional judgment it is believed the informing of the individual would place the individual at risk of serious harm, or
 - b) It is believed that the personal representative being informed (immediate family member or next of kin) is responsible for the abuse, neglect, or other injury and that informing the personal representative would not be in the best interest of the individual as determined by an exercise of professional judgment.
- h. For academic purposes
 - 1) Conducted by an individual or institution that has a formal relationship with the CoC if the research is conducted either:
 - a) By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by the CoC , or
 - b) By an institution for use in a research project conducted under a written research agreement approved in writing by the CoC.
 and
 - 2) Any written research agreement:
 - a) Must establish rules and limitations for the processing and security of personal information in the course of research;
 - b) Must provide for the return or proper disposal of all personal information at the conclusion of the research;
 - c) Must restrict additional use or disclosure of personal information, except where required by law;
 - d) Must require that the recipient of data formally agree to comply with all terms and conditions of the agreement; and
 - e) Is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board, or other applicable human subjects protection institution.
- i. To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
 - 1) In response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer, or a grand jury subpoena;
 - 2) If the law enforcement official makes a written request for personal information that:
 - a) Is signed by a supervisory official of the law enforcement agency seeking the personal information;
 - b) States that the information is relevant and material to a legitimate law enforcement investigation;
 - c) Identifies the personal information sought;
 - d) Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

- e) States that de-identified information could not be used to accomplish the purpose of the disclosure.
 - 3) If it is believed that the personal information constitutes evidence of criminal conduct that occurred on the premises of an HMIS participating agency;
 - 4) In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person and the personal information disclosed consists only of name, address, date of birth, place of birth, social security number, and distinguishing physical characteristics, or
 - 5) If
 - a) 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 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 and 879 (threats against the President and others), and
 - b) 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.
- and
- j. To comply with government reporting obligations for HMIS and for oversight of compliance with HMIS requirements.

D. Accuracy of Personal Information

1. Any individual may inspect and have access to his/her personal information that is maintained in the HMIS. Any questions about information collected can be explained, if necessary.
2. Requests to update or correct personal information are welcome.

To inspect, review, or update information please contact the HMIS Lead Agency at

Big Bend Homeless Coalition
 325 John Knox Rd, Building B
 Tallahassee, FL 32303

Phone 850.576.5566

3. Requests for review or inspection of personal information may be denied if:
 - a. The information was compiled in a reasonable anticipation of litigation or comparable proceedings;
 - b. The information is about another individual (other than a healthcare provider or homeless services provider);
 - c. The information was obtained under a promise or confidentiality (other than a promise from a healthcare provider or homeless services provider) and if the disclosure would reveal the source of the information; or
 - d. Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

4. If a request for access to personal information is denied, a formal explanation must be provided for the denial. Documentation of each request, and denial if necessary, will be maintained in the client file.
5. Repeated or harassing requests may be denied.

E. Data Quality

1. Personal information is collected only for purposes that are relevant for the reasons outlined in section B of this Privacy Statement. To the extent necessary for those purposes, every effort to ensure personal information that is maintained is accurate, complete, and timely.
2. A plan for the deletion/removal of data records has been developed and implemented. Personal information for clients no longer receiving services is removed seven years after the last record of update.
 - a. As an alternative to disposal, identifiable information can be removed so that client records are available for aggregate data purposes only.
3. Information may be kept on file for a longer period of time if required by statute, regulation, contract, or other state or federal requirement.

F. Quality Assurance

1. All questions and complaints about privacy and security policies and practices are reviewed by the HMIS/Data/Performance Committee of the CoC.
 - a. *To file a complaint, an individual must submit, in writing, a description of the grievance. This written complaint must be submitted to the appropriate participating agency (see Appendix) or HMIS Lead Agency who will in turn submit it to the complaint to the HMIS/Data/Performance Committee for consideration. A response to the complaint will be provided within 30 days of its initial submission.*
2. Individuals who work with the HMIS (including employees, volunteers, affiliates, contractors, and associates) are required to comply with this Privacy Statement. Each participating agency will receive a copy of this updated HMIS Privacy Statement to share with individuals who work with HMIS.

G. HMIS Privacy Statement Revision History

1. Version 1.0 – September 30, 2005. Initial Policy Written
2. Version 2.0 – November 7, 2007. Policy Revision
3. Version 2.1 – June 10, 2008. Policy Revision
4. Version 2.2 – August 13, 2009. Policy Revision (Title Change)
5. Version 2.3 – July 30, 2010. Policy Revision
6. Version 3.0 – April 17, 2015. Full Policy Rewrite.