



Safe Harbors HMIS: Privacy Policy

Effective 08/26/2005

Table of Contents



Safe Harbors HMIS: Privacy Policy..... 1

Table of Contents..... 2

Privacy Policy 3

Purpose..... 3

Definitions 3

Client’s Rights 4

Roles and Responsibilities 4

 Safe Harbors Partner Agency Roles and Responsibilities 4

 Safe Harbors Role and Responsibilities..... 4

Policy..... 5

 Safeguarding the Confidentiality of Client Information..... 5

 Personal and Confidential Information on a Web Site 5

 Privacy Training 5

 Background Check..... 5

 Retention of Documentation..... 5

 Privacy Complaints 6

 Corrective/Disciplinary Action for Violations 6

 Actions Prohibited Against Those Reporting Privacy Violations 6

Relationship Termination between Safe Harbors and Participating Agency 6

Privacy Policy

Purpose

This policy describes Safe Harbors privacy practices for safeguarding client confidential information to:

- Promote responsible information management practices by agencies
- Promote public trust and confidence in the use of online services
- Protect the privacy rights of clients when Safe Harbors uses, obtains or discloses information.

Definitions

Client: A person who applies for or receives services from a Safe Harbors partner agency

Client Confidential Information: Personal information that identifies a client, including protected health information, and that state or federal laws protect from improper disclosure or use.

Confidential Information: Information that is protected by state or federal laws, including information about clients that is not available to the public without legal authority.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et seq.

HMIS: Homeless Management Information System — a web based computer system managed by Safe Harbors staff that collects personal information.

Personal Information: Personal information means demographic or financial information about a particular client that is obtained through one or more sources. This may include information such as name, address, social security number, income, education and housing information.

Privacy Policy: Safe Harbors policy developed to comply with Federal and state privacy requirements. The individuals responsible to implement and manage this policy are Safe Harbors staff, Safe Harbors partner agencies, and partner agency staff using the Safe Harbors HMIS.

Safe Harbors: A project jointly funded by City of Seattle, King County and United Way of King County to implement HMIS required by Congressional directive.

Safe Harbors Partner Agency: An agency that signs the Safe Harbors Partner Agency Agreement thereby agreeing to abide by all conditions required of any agency using the HMIS and providing services to homeless people, referred to as clients.

Safe Harbors Privacy Officer: The person who has the primary responsibility for developing and managing the Safe Harbors Privacy Policy.

Safe Harbors Public Disclosure Officer: The person who has the primary responsibility of the Safe Harbors public record disclosure process, including developing, implementing

J:\Safe Harbors 2006\Policies\Privacy Policy V3_d.doc

and overseeing Safe Harbors policies, rules and procedures involved in the disclosure of public records, and for coordinating public records disclosure.

Client's Rights

Clients have the following rights:

- Client's privacy rights are posted in each location in which the HMIS is in place.
- Client has the right to know which agency has added to, deleted or edited their client record.
- Client has the right to refuse to provide personal identifying information, or to stop the agency from entering any personal identifying information into the HMIS.
- Client has the right to decide what personal identifying information can be shared between programs in the Safe Harbors HMIS, and with which it may be shared.
- Client has the right to revoke permission for personal identifying information to be entered or shared in the Safe Harbors HMIS, including what types of information may be shared and with whom it may be shared. Client must notify agency in writing of denial or revocation of data entry and sharing using the HMIS Client Revocation or Denial forms available on www.safeharbors.org or at each Safe Harbors participating program or agency.

Roles and Responsibilities

Safe Harbors Partner Agency Roles and Responsibilities

1. Develop procedures for providing an explanation to clients about the usage of a computerized Homeless Management Information System.
2. All participating agencies agree to abide by all privacy protection standards and agree to uphold all standards of privacy as established by the Safe Harbors.
3. As part of the implementation strategy of the HMIS, a partner agency must have client sharing and release of information procedures and completed forms in place if electronic sharing is to take place.

Safe Harbors Role and Responsibilities

1. Safe Harbors agrees to not use or disclose any identified Client information other than as permitted or required by the Agency Participation Agreement or as required by law.
2. Safe Harbors agrees to use appropriate safeguards to prevent use or disclosure of any identified Client information other than as provided for by the Agency Participation Agreement or as required by law.

3. Safe Harbors agrees to report to Agency any use or disclosure of any identified Client information not provided for by the Agency Participation Agreement of which it becomes aware.
4. Safe Harbors agrees to ensure that any agent, including a subcontractor, to whom it provides identified Client information received from, or created or received by Safe Harbors on behalf of Agency agrees to the same restrictions and conditions that apply through the Agency Participation Agreement to Safe Harbors with respect to such information.

Policy

Safeguarding the Confidentiality of Client Information

Safe Harbors staff and Partner Agency staff must safeguard client confidential information. This includes demographic, financial, eligibility, and protected health information collected, used and stored by Safe Harbors HMIS. Staff must properly safeguard confidential information of past, present and prospective clients from inappropriate use and disclosure.

Staff must follow Safe Harbors policies and procedures in the Safe Harbors Security Policy for handling of confidential data.

Safe Harbors contracts and agreements must contain confidentiality language. In addition, business associate contracts must contain specific confidentiality language addressing the business associates requirements under the HIPAA Privacy Rule.

Personal and Confidential Information on a Web Site

When HMIS gives information about clients or services received, the Internet Confidentiality Notice must be posted on each screen and made available electronically.

Any paper document or export of HMIS data must contain the Confidentiality Notice.

Privacy Training

All Safe Harbors staff must receive annual privacy training related to use, disclosure and collection of client confidential and personal information. Training must be documented in the staff personnel file. New staff must receive privacy training within a reasonable time after being employed by Safe Harbors.

Background Check

All Safe Harbors staff that access client confidential and personal information must undergo a background check.

Retention of Documentation

Safe Harbors must retain the following documentation:

1. Privacy policies and procedures

J:\Safe Harbors 2006\Policies\Privacy Policy V3_d.doc

2. Any written requests or documentation of action or activity relating to clients exercising their privacy rights
3. Privacy complaints and their disposition
4. Documentation that employees have completed privacy training

Safe Harbors must maintain privacy documentation in written or electronic form for six years from the date the document was approved or last revised.

Safe Harbors Agency Partners must retain the following documentation:

1. Agency privacy policies and procedures
2. Any written requests or documentation of action or activity relating to clients exercising their privacy rights
3. Privacy complaints received by agencies and their disposition
4. Safe Harbors User Code of Ethics signed by all agency staff using the HMIS.

Safe Harbors partner agency must maintain privacy documentation in written or electronic form for six years from the date the document was approved or last revised.

Privacy Complaints

Clients believing that Safe Harbors, a Safe Harbors partner agency or Safe Harbors Business Associate has violated a client's privacy rights related to personal or confidential information may file a written complaint with:

1. The Safe Harbors Privacy Officer; and/or
2. The Safe Harbors Executive Committee (roster on www.safeharbors.org)

Corrective/Disciplinary Action for Violations

Safe Harbors staff found to be in violation of Safe Harbors policies and procedures relating to confidentiality of any client information may receive corrective or disciplinary action, up to and including dismissal.

Actions Prohibited Against Those Reporting Privacy Violations

Safe Harbors staff and Safe Harbors partner agency are prohibited from intimidating, threatening, coercing, discriminating against or taking any other retaliatory action toward a client based on their filing of a privacy complaint.

In addition, Safe Harbors may not require clients to waive their right to file a privacy complaint as a condition of receiving services from a Safe Harbors partner agency.

Relationship Termination between Safe Harbors and Participating Agency

1. Safe Harbors shall return, destroy or limit use of any identified client information received, via email, fax, or mailed copy, from the Agency, or created or received by Safe Harbors on behalf of the Agency. This provision shall also apply to Client

information that is in the possession of subcontractors or agents of Safe Harbors. Safe Harbors shall comply with all provisions of the Records Retention Act, RCW 40.14 regarding the management of its records.

2. In the event that Safe Harbors determines that returning or destroying the Client information within the Safe Harbors system is infeasible, Safe Harbors shall provide to Agency notification of the conditions that make that return or destruction infeasible. Safe Harbors would then limit the use of any identified Client information.