

- A brief description of how the individual may file a complaint with the HMIS user or developer.

- 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.

#### 4.5 Rights To Request Privacy Protection for Protected Personal Information

##### Access of Individuals to Protected Personal Information

An individual has a right of access to inspect and obtain a copy of his/her own protected personal information in a record set, for as long as the protected personal information is kept, except for information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. The individual also has the right to correct protected personal information (such as name and date of birth) when that information is inaccurate.

An HMIS user or developer must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected personal information from the HMIS user or developer by alternative means or at alternative locations.

##### Accounting of Disclosures of Protected Personal Information

An individual has a right to receive an accounting of disclosures of protected personal information made by an HMIS user or developer in the six years prior to the date on which the accounting is requested, except for disclosures for national security or intelligence purposes or to correctional institutions or law enforcement officials.

The HMIS user or developer must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, for the time specified by such agency or official, if the agency or official provides the HMIS user or developer with a written statement confirming that such an accounting would impede the agency's activities. The notification should specify the time for which such a suspension is required.

#### 4.6 Administrative Requirements Local Protocol

A CoC system administrator is required to have a written policy governing its use and disclosure of information collected by HMIS. This policy should address the specifics of how use and disclosure decisions will be made and who will make them and with what documentation, as well as the specifics of how the data security standard will be met. These decisions should include who will have access to HMIS data and the level of access granted to each user. The policy should also address grievance procedures and penalties for non-compliance. Examples of such policies are discussed in the HMIS Implementation Guide available on HUD's Web site.

To test system and application security, a CoC system administrator is encouraged to periodically conduct penetration testing, a procedure which is also described in the Implementation Guide.

##### Local Policies

A CoC system administrator or developer who has instituted policies in addition to those listed in this notice must maintain a written copy detailing any and all additions and specifications beyond the content of this notice. Such written policy must be distributed to all staff and included as an additional notice for individuals affected.

##### Safeguards

A CoC system administrator or developer must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected personal information including, but not limited to, those described in this notice and required by law.

##### Training

A CoC system administrator user or developer must provide orientation and ongoing training to all of its staff on the policies and procedures relating to protected personal information sufficient for staff to carry out their functions.

#### 5. Technical Standards

This section presents the technical standards that will be required for HMIS applications and for the CoCs responsible for storing HMIS data. Except as otherwise provided, these standards do not specify or recommend any particular operating system, development environment, networking environment, database, hardware, or other aspect of the HMIS application.

This part of the notice is primarily directed to HMIS developers and CoC system administrators.

#### 5.1 Required HMIS Capabilities

##### Automatic Generation of Identification Numbers and Information

Based on the data collected through program staff interviews or self-administered forms, the HMIS application must be capable of automatically generating data for each record. This capability includes the automatic generation of:

- (1) Unique personal identification numbers (PINs) for persons who have not been previously served within the CoC, and re-assignment of PINs for persons who have been served previously within the CoC;
- (2) Household identification numbers for persons who have been identified as members of a household that participated in the same program event;
- (3) Program identification information that is uniquely associated with each program within a CoC and is assigned to every program event; and,
- (4) A program event number that distinguishes each episode of program utilization.

##### Personal Identification Numbers (PINs)

PIN is a number randomly and automatically generated by the HMIS application. All records associated with the same person should be assigned the same PIN. The PIN is used to produce an unduplicated count of all persons within a CoC.

HMIS must be capable of searching the entire CoC database (whether or not data are shared across programs within a CoC) to determine if clients have been previously served. The search must involve the matching of client records using personal identifier fields (*e.g.*, Name, Social Security Number, Date of Birth, and Gender) to retrieve a record(s) with identical or similar values in each of these fields.

##### Household Identification Numbers

HMIS must generate the same household identification number for every person designated by program staff as being together for an episode of service (*i.e.*, program event). The household identification numbers assigned will be maintained in each person's permanent record and will be unique for each program event experienced by the client.

As discussed in Parts 2 and 3 of this notice, when a group of persons apply for services together (as a household or family), information is first asked of the household head who is applying for services and then information is