DUFFERIN
COUNTY

HIFIS - Privacy and Confidentiality Considerations

Client Consent

- All clients must give signed, informed consent before their information can be added to HIFIS.

- There are three different types of consent in HIFIS:
  1. Explicit (recommended for data sharing purposes)
  2. Inherited (for dependents who are not of age to consent)
  3. Declined – Anonymous ("Declined" will hide a client from being accessed by other service providers. This option may result in the client having more than one record in HIFIS).

- A scanned copy of the signed consent form can be uploaded into HIFIS.

- Consent ensures clients are made aware of the ways their information will be shared and used before agreeing to give their information, and confirms service providers are complying with privacy laws.

- Once a client provides consent to have their information recorded in HIFIS, that consent is good for two years and is valid unless the client indicates they would like to withdraw it.

Clusters

- While the intent is to have a single client record in HIFIS for each client and to share this record among service providers, it is recognized that in some cases this is not appropriate.

- Clusters were developed in HIFIS so that some service providers and their clients can be separated into different groups. Clients served by service providers in a cluster can only be viewed by service providers in that same cluster. The majority of service providers and their clients will be in the main cluster which is called the "Integrated" cluster. Other clusters can be created as needed.

Limiting Access to client files

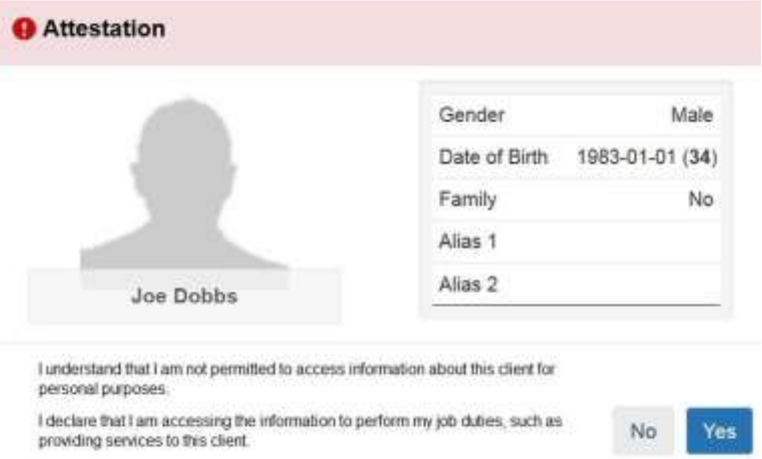
- Service Provider visibility settings can be set based on gender and age. For example, a women's shelter can be set up to ONLY view female clients in HIFIS and a youth shelter can be set up to view clients only under a certain age. Users who log in at a service provider will be unable to access clients that don't meet the visibility criteria set for the provider.

- A Service Provider can also choose to hide all of their data from all other providers (this option is set up by Administrator)

- Client lists within HIFIS can also be restricted (not displayed) so that ONLY searches can be performed to access clients. The User will need to know the name of the person they are looking for in order to access a file.

Attestation

- Once a client's record is created, it will be available to users at other sites in the same cluster. Prior to viewing and working with the client record, users at other sites will have to attest that they have a valid reason for accessing it. HIFIS will prompt all users to provide attestation the first time they go into a client's record. The screenshot below shows the screen presented.



Attestation

Joe Dobbs

Gender	Male
Date of Birth	1983-01-01 (**34**)
Family	No
Alias 1	
Alias 2	

I understand that I am not permitted to access information about this client for personal purposes.

I declare that I am accessing the information to perform my job duties, such as providing services to this client.

User Rights

- Users are given a set of system "rights" for each site they work at. A user's rights grant or restrict access to HIFIS modules and sub-modules. For example, rights can be granted to allow access to a client's record and their shelter stays, but not to their case plans. Rights can also be set to specify if a user can create, edit or view records.

Secure Passwords

- Once a New User has been signed up to HIFIS, HIFIS will email the User directly to prompt them to create a secure password (this way their password is kept from all others, including Administrator).

- In case of a forgotten password, no hints are provided and no "secret questions" are used to prompt new passwords. HIFIS will email a password recovery link to the User.

- Passwords must be a minimum of 8 characters (can be revised by Administrator), and the Password age limit has been set for 120 days (can be revised by Administrator)

Network Security

- Access to the HIFIS Database is limited to Users on an approved network only.

“Shareable” Toggle

- Several Client Information records within HIFIS may contain sensitive information that will not be shared amongst sites. These include:
    - Health issues (Client Information > Health Information > Health Issue)
    - Medication information (Client Information > Health Information > Medication)
    - Financial information (Client Information > Financial Profile)

- Any time a record is entered in one of these modules the Shareable toggle will be set to ‘No’ (by the User) to prevent it from being shared amongst sites. By default, all Shareable toggles are set to No. An audit report exists that will identify any records that are being incorrectly shared

Staff Training

- All HIFIS Users will sign and agree to a HIFIS User and Confidentiality Agreement outlining their responsibilities in handling the confidential information contained in HIFIS

- All HIFIS Users will be appropriately trained on protecting client information. Privacy and confidentiality issues are covered in the HIFIS User Manual, the HIFIS New User training presentation, and in several supporting documents.

- All staff will receive training on privacy breaches – including what constitutes a privacy breach, and what actions should be taken should a breach in privacy happen.

Audit Logs

- All actions taken by HIFIS users are recorded in a system audit log. Several reports are generated from the audit log, which can be reviewed by Administrators on a regular basis to ensure users are not inappropriately accessing client records