FAQ: Client Consent and HMIS Release of Information

A **Client Consent to Data Collection and Release of Information (ROI)** must be completed for each client who consents to have their personally identifying information (PII) entered into the King County HMIS System. The form can be signed two ways:

1. **Electronically**: A client can consent by reviewing and signing the ROI form electronically in HMIS. For more information,
2. **Hard copy upload**: A client can consent by reviewing and signing a paper version of the ROI and having the service provider scan and upload the signature page into the HMIS. A PDF version of the ROI form for printing and signing can be found on the King County HMIS website

The King County HMIS End User Manual includes detailed instructions on the ROI process. also includes instructions on how to enter de-identified information for clients who do not consent, or for whom de-identified PII is required, such as clients actively fleeing domestic violence and clients disclosing their HIV status within HMIS.

COVID-19 Temporary HMIS Consent Policies - Effective March 25, 2020CO

1. **Can I obtain verbal consent to enter and share a client's PII in HMIS?**
   Yes. King County HMIS policies now temporarily allow for verbal consent and release of information due to the COVID-19 crisis. Staff must explain the information contained in the Client Consent to Data Collection & ROI (2020) and Client Information Sheet, and answer any questions from client to allow for meaningful informed consent before asking client to consent, and before creating a client profile in HMIS that contains personally identifying information (PII), such as Name, SSN, and Date of Birth. (Note: additional languages other than English can be found on HMIS Webpage)

   If verbal consent is granted by the client, the client's consent must still be documented in HMIS behind Privacy Shield in HMIS by marking "verbal consent" (see screenshot below). The verbal consent may be in place until the staff is able to obtain a signed ROI for uploading into HMIS at the next available opportunity when in-person contact can happen.

   As part of collecting or verifying the identifying information over the phone, staff should be sensitive to any concerns re: safety/domestic violence and must never release/verify to caller any information that the staff person is seeing in HMIS...even if caller has shared PII that matches what is currently showing in HMIS.

2. **What if I don't have immediate access to a scanner in my new remote work situation in order to scan and upload a paper ROI Form?**
   Since staff complying with new social distancing work locations may no longer have a convenient way to scan and upload a PDF into HMIS, they may now temporarily keep the paper ROI Form on file until upload can happen. To indicate that the client has provided a signed consent form and the staff has the paper copy in possession, the staff should select "Signed Paper Document" as the option when Adding ROI behind the Privacy Shield. Staff must keep the paper copy of the signed ROI in a secure location approved by the Agency until staff are able to scan and upload the PDF per usual.

FAQ: Client Consent and HMIS Release of Information

Obtaining and Documenting Consent

3. **Am I required to obtain an ROI from a client?**
   Yes. When creating a new client profile in HMIS, all providers are required to document whether a client consents to sharing identifying information in HMIS. For clients who consent, an ROI must be electronically signed or uploaded via "Add a Release of Information" link in HMIS. Not only does this ROI provide legal documentation of a client's consent, having identifying information in HMIS allows providers to more easily serve clients, better obtain a picture of services clients are receiving across the continuum, and assist in the documentation of chronic homelessness.

4. **Is it okay to scan and upload the signature page only?**
   Yes. Where the ROI itself is a multi-page document uploading just the signature page of the ROI is acceptable.

5. **Is there a way to track verbal consent?***
   No. Consent must be documented through a signed ROI. The ROI can be electronically signed or uploaded into HMIS by clicking the "Add Release of Information" link under a client's Privacy Shield icon.

6. **How do I know whether my client has an ROI on file?**
   Locate the client's profile in the system and click on the Privacy Shield icon. Existing ROIs will be listed In the Release of Information section. If the section says, "There are no results to display," this means that the client does not have an ROI on file.

7. **Who is responsible for adding the ROI?**
   The agency who initially enters client information into HMIS is responsible for documenting consent status in HMIS, and for adding the ROI for clients who consent.

8. **Does every agency need to complete an ROI for every client they work with?**
   No. A client should only be asked to complete the ROI one time; client information is stored for 7 years after the last recorded service in HMIS.

9. **What do I do if my client's profile contains identifying information (name, SSN, exact DOB), but no ROI has been added?**
   If no ROI has been added for an identified client, you should contact the most recent agency serving this client to obtain a copy of their ROI, or request that the agency add their ROI to HMIS. If that is not feasible, then you should confirm consent with your client and enter the ROI. Any agency serving the client before 2016 should have a signed ROI on file since ROIs under the previous HMIS were not shared across the continuum and were not uploaded into HMIS. If a client no longer consents, you **must never attempt** to de-identify the client record. Clients records must only be de-identified by the Bitfocus Helpdesk after the client signs a Revocation of Consent orm.

FAQ: Client Consent and HMIS Release of Information

Families and ROI

10. **Does every member of a household need to complete a separate ROI?**
    Yes. Each household member must sign an individual ROI. Parents can sign for children under 18. Each ROI should be added under the individual family member's Privacy Shield. Only *unaccompanied* youth aged 13 through 17 can sign an ROI for themselves. When they are with a parent or guardian, the parent or guardian will sign for them. Client identity could be determined through the identities and relationships of family members. Therefore all members of a family must be deidentified if consent is refused for any one member.

11. **Should a teenager who is part of a household sign their own ROI once they turn 18?**
    Yes. The individual client who turned 18 years old should now sign their own ROI to replace the version signed by the parent/guardian when the individual was a minor. The client can remain part of the household in HMIS like any other adult household member.

12. **What if some family members are identified and my client declines consent for themselves or their child?**
    If a client declines consent, but their family members are already identified in the system, have them or the identified member (if adult) sign a revocation of consent form. Then contact the Help Desk to have them de-identified. Client identity could be determined through the identities and relationships of family members. Therefore all members of a family must be deidentified if consent is refused for any one member.

13. **Can a client sign the ROI for their spouse?**
    No. A client may only sign the ROI for themselves and for their children who are under the age of 18.

Veteran Affairs ROI

14. **Do veterans need to complete a VA ROI?**
    Veterans need to complete a VA ROI in order to be considered for certain housing programs for veterans. The VA ROI is currently only available in hard copy and cannot be electronically signed within HMIS. Ideally, the HMIS ROI and the VA ROI should be scanned and uploaded as one document under the client's Privacy Shield. If that's not possible, the HMIS ROI should be added under the Privacy Shield and the VA ROI should be uploaded under the client's Files tab.

15. **What if my client chooses to sign the HMIS ROI electronically? How do I handle the VA ROI?**
    Since only one ROI can be added under the Privacy Shield, the VA ROI should be scanned and uploaded under the client's Files tab. Instructions for using the Files tab can be found via the Clarity Human Services Help Center.

16. **What if my client already has an HMIS ROI added under their Privacy Shield but I need to add a VA ROI?**

Since only one ROI can be added under the Privacy Shield, the VA ROI should be scanned and uploaded under the client's Files tab. Instructions for using the Files tab can be found via the Clarity Human Services Help Center.

17. **Does every member of a veteran's household need to complete a VA ROI?**
    No. Only the veteran needs to sign a VA ROI.

18. **Don't all veterans enrolled in SSVF programs HAVE to consent since the VA requires PII in order to verify a person's veteran status?**
    No. A client can always decline to have PII stored and shared in HMIS. However, if the VA doesn't have a name/SSN then the VA cannot confirm that the client is a veteran. It is important for SSVF programs to review the timing of revocations (ie, has this client been reported to the VA already or not), and to engage the VA Regional Coordinator ascertain whether alternative data collection measures will be needed to account for client data uploads. If the year in which the client was served has passed, it might not be an issue for the VA anymore in terms of the name being in HMIS, but client files will always need to be up-to-date and accurate for monitoring purposes.

Non-Consenting Clients and Revoking Consent

19. **When do providers need to sign the ROI?**
    A provider only needs to sign the ROI when a participant is non-consenting. Although non-consent must still be documented under the client's Privacy Shield (as "No"), the ROI form for a non-consenting client is not entered into the system but is instead kept on file at the agency documenting the consent status.

20. **What if my client wants to revoke their consent to having identifying information entered in HMIS?**
    A client may revoke consent by completing and signing the Client Revocation of Consent form. The agency must then contact the Bitfocus Helpdesk and request that the client record be de-identified. The Helpdesk may ask a few questions to ensure that all protocols are being followed and/or may direct you to work with Coordinated Entry Entry for All if your client is awaiting a housing referral via the Community Queue. Make sure your client has their Clarity Human Services Unique Identifier to provide to other providers in order to avoid creation of duplicate records.

21. **Can I de-identify my client's profile after they've signed the Revocation of Consent form?**
    No. To ensure that all client data in HMIS is correctly de-identified, and that all providers (including Coordinated Entry for All staff) working with the client are notified, you **must** contact the Bitfocus Helpdesk when a client needs to be de-identified.

22. **What if a client tells me they don't consent but I see that they have an ROI entered into HMIS?**
    If a client has an ROI entered into HMIS, the client is considered consenting until they complete and submit a Revocation of Consent form. The Revocation of Consent form is available on the King County HMIS website.

23. **What if I see that my non-consenting client has another identified profile in the system?**
First, determine whether the identified profile has an ROI entered in HMIS (look for a record in the Release of Information section under the Privacy Shield in your client's profile). If the client has a consenting ROI that's dated more recently than your non-consenting ROI, the client is considered consenting until they submit a Revocation of Consent form. If your non-consenting ROI is newer, that ROI takes precedence and the client should remain de-identified. Once you've determined whether the client should be identified or de-identified in the system, you can contact the Bitfocus Helpdesk to have the two profiles merged, keeping either the identified or de-identified profile as appropriate. If the client will be de-identified in the system, make sure they have their Clarity Human Services Unique Identifier to provide to other providers in order to avoid creation of duplicate records.

De-Identified Populations

24. **What do I do if my client is actively fleeing a domestic violence (DV) situation?**
If your program is a Victim Service Provider you should never enter identifying information for any client served by your program. No personally identifying information may be entered for any client *actively fleeing* domestic violence (in compliance with the Violence Against Women and Department of Justice Reauthorization Act of 2005 (VAWA) and Washington State RCW 43.185C.030). If you are providing services for a client who is actively fleeing domestic violence you must create a new, de-identified profile for your client, regardless of whether they have an existing profile in the system. The profile you create should only be used by your agency and no effort should be made to merge or de-duplicate this profile with any other in HMIS. To enter a de-identified profile, follow the process outlined in the King County HMIS User Manual.

If your program is NOT a Victim Service Provider but you are providing services for a client who is actively fleeing domestic violence, you should assist the client in making an informed decision about whether having identifying information in HMIS could compromise their safety. In some cases it may be appropriate to create a new, de-identified profile for your client to only be used by your program, regardless of whether they have an existing profile in the system. To enter a de-identified profile, follow the process outlined in the King County HMIS User Manual. If your client is now actively fleeing domestic violence and wants to revoke consent after previously consenting, immediately contact the Bitfocus Helpdesk to have the profile de-identified. The client **does not** need to complete a Revocation of Consent form. If the client chooses to not consent to having identifying information in HMIS, they may still wish to provide their Clarity Human Services Unique Identifier to other providers in order to avoid creation of duplicate records.

25. **What do I do if my client is disclosing their HIV+ status within HMIS?**
Unless you are enrolling a client in a HOPWA-funded program, it is not necessary to document HIV status in HMIS and thus not a requirement to de-identify your client. However, if you are enrolling your client in a HOPWA-funded program, no personally identifying information may be entered for any client whose

HIV+ status is being documented in HMIS (in compliance with RCW 70.02.220). If you are creating a new profile for a client whose HIV+ status is being disclosed in HMIS, follow the process outlined in the User Manual to create a de-identified profile for your client. If your client already has a profile containing identified information, contact the Bitfocus Helpdesk to have the profile de-identified. The client **does not** need to complete a Revocation of Consent form. Be sure to provide your client with their Clarity Human Services Unique Identifier to help other agencies locate their profile in order to avoid creation of duplicate records.

26. **What do I do if my agency or program is known in the community to only serve HIV+ clients?**
If your program has been identified by King County as one who should follow a special protocol, then you will be instructed to never enter identifying information for any client served by your program. No personally identifying information may be entered so that a client's HIV status cannot be inferred by affiliation with your program. The profiles you create should only be used by your agency and no effort should be made to merge or de-duplicate this profile with any other in HMIS. To enter a de-identified profile, follow the process outlined in the King County HMIS User Manual.

27. **What do I do if I serve unaccompanied youth (under 18)?**
Beginning June 7, 2018: Any unaccompanied youth aged 13 or older may consent to have their personally identifying information collected for the purposes of HMIS. The term unaccompanied is defined as a youth or young adult experiencing homelessness while not in the physical custody of a parent or guardian.

28. **What happens when a parent/Guardian disagrees [with minor youth] about whether to consent to HMIS or not? Does the Guardian's decision about HMIS consent trump the minor's decision?**
The consent change is for unaccompanied youth only, so if a minor is in a household with a parent or guardian, they decide whether or not to consent for the entire household. A parent or guardian isn't present in unaccompanied youth households.

29. **Does an individual (who has consented as a minor) need to re-sign the HMIS consent form as an adult? (Do they need to re-sign the consent upon turning 18)?**
No. The consent form is the same for Unaccompanied Youth and Adults. Client information is stored in the database for 7 years after the last date of service is recorded in HMIS.

30. **Should I use the same HMIS consent form for minors as we do for adults?**
Yes

31. **Is there a Youth-specific HMIS consent form developed that provides the same info in simple, youth-focused language?**
No. There should always be a conversation about HMIS with the person being served (youth or adult) to ensure the client understands the information, and has the opportunity to ask questions.