

HPRP/HMIS Tip of the Week 5

Anonymous Clients, Client Privacy

Privacy is one of the main concerns many people have about a centralized database such as HMIS, especially because we are entering personal data on a vulnerable population. A client's decision about his/her participation in HMIS should never be a barrier to the client receiving help.

HPRP's privacy guidelines are based on "implied consent", which means at intake, the client does not need to sign a Release of Information form as long as a privacy statement is posted in plain view of the client at intake. However, any client who indicates that they are domestic violence clients should be entered as anonymous, regardless of any kind of consent. This treatment of domestic violence clients applies across all programs, not just HPRP.

Further, for any client who wishes it, there is the option of entering the client into ServicePoint as Anonymous. This option is not ideal, because it defeats an important feature of HMIS, which is to unduplicate clients across agencies and episodes. Anonymous clients are duplicated at least across agencies, because other agencies searching for your anonymous client will not find them since they will not know their client ID. It is also possible the client could be duplicated within the same agency if your physical files do not reference the client's ID number in ServicePoint or if a case manager just didn't know to look for the client's ID. This kind of data duplication can cause inaccurate reporting. So, as a case manager, you will want to explain to the clients who are on the fence about data sharing his/her privacy rights, but also explain to them how having their personal data helps your agency and homeless folks in general, since your reporting goes to Congress and decisions are made about the homeless population based on this data.

Nevertheless, there will be clients who should, without question, be entered as anonymous, and it is certainly more important for these clients to be safe than our reporting to be perfect. Again, domestic violence clients will always go into HMIS as Anonymous, and anyone else who has safety concerns should not be pressured into giving their personal data. So, here, I will briefly explain how to enter a client as Anonymous. Simply go to ClientPoint, slide to the bottom of the search screen and click Add Anonymous Client.

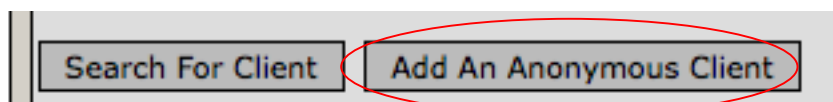


Figure 1: Add an Anonymous Client

The database will create a client with a Client ID number, a first name of "Anonymous", and a compiled last name similar to Figure 2:



Figure 2: Anonymous client

It is a good idea to write down your client ID for your anonymous clients especially, because there is no other way to find anonymous clients in the database. For anonymous clients, you should enter Refused for SSN, birth date, and anything else that would personally identify that person. Everything else will be the same. Housing Status, income, non-cash, service transactions, etc. should all be answered whether anonymous or not.

Now that you understand the nuts and bolts of entering a client as anonymous, I would like to give a baseline for privacy standards for all HPRP programs covered under the Balance of State. Please call or email if there is something here that you do not understand.

- Do not share your username/password with another person for any reason. All users who log into ServicePoint should be using their own login and password at all times.
- Do not write down your password.
- Choose strong passwords, not something that could be guessed just from knowing you. When I worked in I.T., I would sometimes need to guess at passwords when people weren't around but I needed to do something on their computer. About 90% of the time, I could guess the password only from knowing a tiny bit about that person, even just including what they decorate their desks with. It's really that easy. A good idea is to use something that is familiar to you but substitute numbers for some of the letters. Like instead of "nicholas98", you could make it "N1ch0l@s98". The second password is much stronger than the first, but you can still remember it. Another idea is to choose something you find easy to remember, then shift your hands up or down or to the left or right on the keyboard and type as if your hands are in the right place. So instead of "nicholas98", it would be "Buxgika87" or something like that.
- Do not print or email client names, SSNs, or birthdates unless you are printing something that will stay in that client's physical folder in a secure filing cabinet. If you do need to print a report with sensitive client data on it, please shred it when you are done using it.
- When emailing co-workers or anyone (like me, for instance) about a client, please use the Client ID instead of the name. [Email is not secure.](#)
- Agency administrators should make sure that all volunteers, employees, affiliates, and contractors who enter or view client data have signed User Agreements. These User Agreements are all filed at COHHIO.
- Agency administrators, ensure that your network is behind a firewall and that any computer used for HMIS data entry has updated virus protection.
- Agency administrators, please be very diligent about keeping COHHIO informed of any staff changes that involve ServicePoint users. Ex-employees/volunteers/contractors need their accounts inactivated immediately after leaving their positions so that there are no extra logins out there that no one is accountable for.

It is easy to get complacent and feel totally comfortable with bits of people's data lying about, passwords posted right on the monitor, but should any data get out to the wrong person/entity about a client, then this system, your agency, our work will have failed in its intent to help (and not hurt) our clients. Many feel that some clients are careless about their data in other ways, through using credit cards or having internet accounts or receiving food stamps or checking out books from a library, and these things may be true, but it cannot be assumed. We do not want our agency, our HMIS to be the weak link that is going to end up hurting a client. Also, this data is kept for *seven years* after the data was last edited. This leaves many who have worked their way out of homelessness in a vulnerable position, as data from their past could get into the wrong hands and hurt them later on. These are some of the reasons it is so important to follow all the HUD guidelines on keeping your client data secure.

Privacy is a vast topic, and I have only covered some of the points I feel are most relevant to you. This is not meant to be a comprehensive guide to privacy, and it is recommended that you read the [2004 Data Standards](#) for more details on privacy. (Start at page 9 of the pdf.)

Comments, questions, and feedback are welcome. If you would like to not receive HPRP HMIS Topic of the Week anymore, or would like to be included, please email genelledenzin@cohhio.org.