Data Privacy and Confidentiality in CAPV's CMS (CHPM) Database System

Community Action Pioneer Valley (CAPV) takes the privacy and confidentiality of our clients and participants (including employees that are also clients) seriously.

All CAPV employees are required to adhere to **CAPV's Confidentiality Policy**, which is included in the CAPV Personnel Handbook and is excerpted below.

The individual dignity of clients/participants and employees shall be respected and protected at all times. All employees will be required to sign a Confidentiality Statement upon hire. Information about clients/participants or Community Action/HS & ELP business must not be divulged to anyone other than persons who are authorized to receive such information. This policy extends to both internal and external disclosure.

Confidentiality of Participants', Children's, and Families' Information:

- *All clients'/participants' records must be locked in a secure file.*
- *Access to clients'/participants' records is limited to employees on an as-needed and appropriate basis.*
- *Clients'/Participants' records must not be removed; however, copies can be made for purposes of audit, investigation, family needs, school transition, or as otherwise needed as consistent with state and federal law.*
- *Clients'/Participants' records must never be left on desks, tables, etc. where others have access to them.*
- *Clients'/Participants' private information must never be discussed among employees except on a "need to know" basis. Employees must be particularly aware of their surroundings when discussing this information. Special caution must be taken to be sure other clients/participants or employees do not overhear information that is private.*
- *Discussion of clients'/participants' information with volunteers, other clients/participants, friends, or community members is prohibited.*
- *Information and documents which are considered confidential are medical records, educational records, special needs records, family records, financial records, and any other private information about clients/participants, their families, or Community Action/HS & ELP business.*
- *All requests for the release of information will be coordinated by a designated program employee and will comply with applicable laws.*
- *Identifiable information will only be released in accordance with state and federal confidentiality laws.*

Violation of Confidentiality Policy: Any employee who violates the Confidentiality Policy will be subject to disciplinary action, up to and including termination

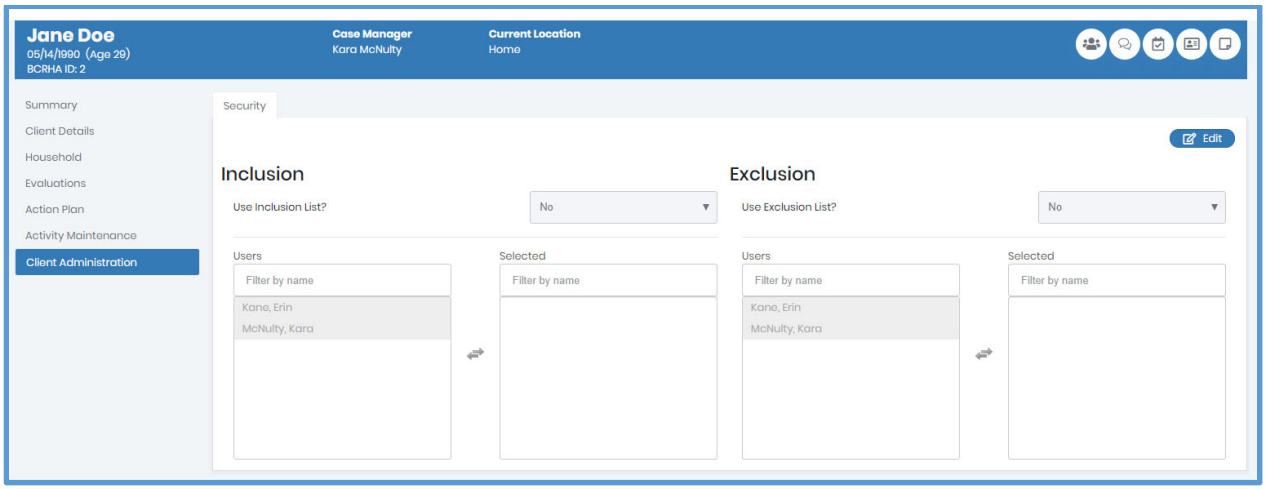
Inclusion/Exclusion Security Setting

CMS database has a setting that allows the Agency Admins to protect certain client data in the system from being widely viewed by all CMS users.

Excerpt from the User Guide

Client Administration

The Client Administration screen allows you to manage inclusion and exclusion based security. Please note that only users with the proper permission will have the ability to view and edit this screen.



1. *Security Definitions*
    a. ***Inclusion Security** is used to only allow a select number of users to view the client. Only the selected users on the Inclusion list will have the ability to access this client's record. An example of when an inclusion list may be used is when a staff member at an agency is also a client.*
    b. ***Exclusion Security** is used to restrict specific users from viewing a client. Any user who is on the exclusion list will not have the ability to access the client's record. An example of when an exclusion list may be used is when a staff member has had issues with a client in the past and a client has requested to not work with that specific staff member.*

These settings can be applied to:

- CAPV employees and members of their households who are clients of CAPV program(s) *(inclusion security)*
- Clients with extremely sensitive data needs that if compromised could result in a serious threat to safety *(inclusion security)*
- Family members of CAPV employees that request that their data be restricted from specific employees (i.e. Susie's sister works at CAPV and she does not want her sister to see her client record) *(exclusion security)*

Frequently Asked Questions

How can employees request this setting?

CAPV employees may opt into either security setting at any time by emailing the CMS Agency Admins Cynthia DiGeronimo (cdigeronimo@communityaction.us) or Janna Tetreault (jtetreault@communityaction.us). Employees must identify which security setting they are requesting.

The Agency Admins will keep track of which CAPV employees have opted in, which setting is applied and to whom (list of household members), and who has access to their record.

Information about this setting, including a link to this document, is included at the bottom of the CAPV Permission to Release Information.

How can a client request this setting?

Clients may request this setting at the time of Program Enrollment. The CAPV employee working with the client will send an email request to the Agency Admin(s) to make the request.

How will the protected data appear in CMS?

Client data (name and Agency ID) will appear in the Search Results to prevent duplication but employees will not be able to select the client to review their record. This setting can be applied to all members of the household or just one member of the household.

If only one member's record is protected (i.e. a youth participating in Youth & Workforce Development), the services that they receive will appear under the Household Action Plan screen. The only protected data is the data in Client Details.

Who can open the Client Record?

If using the *inclusion security setting,* all staff will be able to see that the employee has a Client Record in CMS but only a select group will be able to open it. Agency Admins will always have access to the Client Record. If the client is actively engaged in a Program, the Agency Admins will determine with Program staff who needs access to the Client Record to provide services. At a minimum, it would be the Case Worker and the Supervisor for that Program. The CAPV employee will not have access to his or her Client Record or the Client Records of their household members.

If using the *exclusion security setting*, all employees will be able to see and open the Client Record except for the specific CAPV employee identified to exclude. In that case, that employee can see the record but cannot open it.

A new client applies to my Program and when I search their record, I cannot open it. What do I do?

This may happen when a Client (either a CAPV employee, a member of their household, or a non-employee client) who previously obtained services from CAPV

and opted to protect their data seeks a new service. In this case, please contact the Agency Admins to add the appropriate employee(s) to the *inclusion security setting*. The Agency Admins will also reach out to the CAPV employee to notify them that there is a change to their setting to provide them with services. Program staff will notify the non-employee client that there is a change in the security setting.