



Privacidad y confidencialidad de datos en el sistema de base de datos CMS (CHPM) de CAPV

Community Action Pioneer Valley (CAPV) toma en serio la privacidad y confidencialidad de nuestros clientes y participantes (incluidos los empleados que también son clientes).

Todos los empleados de CAPV deben cumplir con la **Política de Confidencialidad de CAPV**, que se incluye en el Manual del Personal de CAPV y se resume a continuación.

La dignidad individual de los clientes/participantes y empleados será respetada y protegida en todo momento. Todos los empleados deberán firmar una Declaración de Confidencialidad al momento de la contratación. La información sobre los clientes/participantes o los negocios de Community Action/HS y ELP no debe divulgarse a nadie más que a las personas autorizadas para recibir dicha información. Esta política se extiende tanto a la divulgación interna como externa.

Confidencialidad de la información de los participantes, los niños y las familias:

- *Todos los registros de los clientes/participantes deben estar guardados en un archivo seguro.*
- *El acceso a los registros de los clientes/participantes está limitado a los empleados según sea necesario y apropiado.*
- *Los registros de los clientes/participantes no deben eliminarse; sin embargo, se pueden hacer copias con fines de auditoría, investigación, necesidades familiares, transición escolar o según sea necesario y consistente con las leyes estatales y federales.*
- *Los registros de los clientes/participantes nunca deben dejarse en escritorios, mesas, etc., donde otros tengan acceso a ellos.*
- *La información privada de los clientes/participantes nunca debe discutirse entre los empleados, excepto sobre la base de la "necesidad de saber". Los empleados deben ser particularmente conscientes de su entorno cuando discutan esta información. Se debe tener especial precaución para asegurarse de que otros clientes/participantes o empleados no escuchen información privada.*
- *Conversar sobre información de los clientes/participantes con voluntarios, otros clientes/participantes, amigos o miembros de la comunidad está prohibido.*
- *La información y los documentos que se consideran confidenciales son registros médicos, registros educativos, registros de necesidades especiales, registros familiares, registros financieros y cualquier otra información privada sobre clientes/participantes, sus familias o negocios de Community Action/HS y ELP.*

- Todas las solicitudes de divulgación de información serán coordinadas por un empleado designado del programa y cumplirán con las leyes aplicables.
- La información identificable solo se divulgará de acuerdo con las leyes de confidencialidad estatales y federales.

Violación de la Política de Confidencialidad: Cualquier empleado que viole la Política de Confidencialidad estará sujeto a medidas disciplinarias, hasta e incluyendo el despido

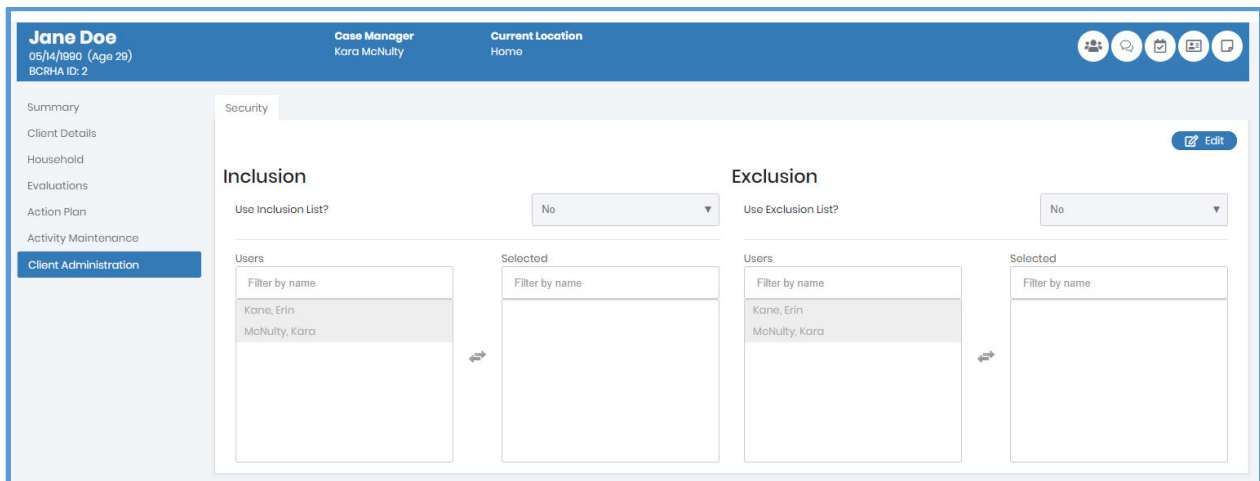
Configuración de seguridad de inclusión/exclusión

La base de datos CMS tiene una configuración que permite a los administradores de la agencia proteger ciertos datos de cliente en el sistema para que no sean ampliamente vistos por todos los usuarios de CMS.

Extracto de la Guía del Usuario

Administración de Clientes

La pantalla Administración de Clientes le permite gestionar la seguridad basada en la inclusión y la exclusión. Tenga en cuenta que solo los usuarios con el permiso adecuado tendrán la capacidad de ver y editar esta pantalla.



1. Definiciones de seguridad

- Seguridad de inclusión** se utiliza para permitir que solo un número seleccionado de usuarios vea el cliente. Solo los usuarios seleccionados en la lista Inclusión tendrán la capacidad de acceder al registro de este cliente. Un ejemplo de cuándo se puede usar una lista de inclusión es cuando un miembro del personal de una agencia también es un cliente.
- Seguridad de exclusión** se utiliza para restringir a usuarios específicos la visualización de un cliente. Cualquier usuario que esté en la lista de exclusión no tendrá la capacidad de acceder al registro del cliente. Un ejemplo de cuándo se puede utilizar una lista de exclusión es cuando un miembro del personal ha tenido problemas con un cliente en el pasado y un cliente ha solicitado no trabajar con ese miembro del personal específico.

Estos escenarios se pueden aplicar a:

- Empleados de CAPV y miembros de sus hogares que son clientes del (de los) programa(s) de CAPV (*seguridad de inclusión*)
- Clientes con necesidades de datos extremadamente sensibles que, si se ven comprometidos, podrían resultar en una amenaza grave para la seguridad (*seguridad de inclusión*)
- Familiares de empleados de CAPV que solicitan que sus datos sean restringidos a empleados específicos (es decir, la hermana de Susie trabaja en CAPV y no quiere que su hermana vea su registro de cliente) (*seguridad de exclusión*)

Preguntas frecuentes

¿Cómo pueden los empleados solicitar esta configuración?

Los empleados de CAPV pueden optar por cualquier configuración de seguridad en cualquier momento enviando un correo electrónico a los Administradores de la Agencia CMS, Cynthia DiGeronimo (cdigeronimo@communityaction.us) o Janna Tetreault (jtetreault@communityaction.us). Los empleados deben identificar qué configuración de seguridad están solicitando.

Los Administradores de la Agencia realizarán un seguimiento de qué empleados de CAPV han optado, qué configuración se aplica y a quién (lista de miembros del hogar), y quién tiene acceso a su registro.

La información sobre esta configuración, incluido un enlace a este documento, se incluye en la parte inferior del Permiso de CAPV para Divulgar Información.

¿Cómo puede un cliente solicitar esta configuración?

Los clientes pueden solicitar esta configuración en el momento de la inscripción al programa. El empleado de CAPV que trabaja con el cliente enviará una solicitud por correo electrónico a la(s) Agencia(s) Administradora(s) para realizar la solicitud.

¿Cómo aparecerán los datos protegidos en CMS?

Los datos del cliente (nombre e ID de agencia) aparecerán en los Resultados de Búsqueda para evitar duplicaciones, pero los empleados no podrán seleccionar al cliente para revisar su registro. Este ajuste se puede aplicar a todos los miembros del grupo familiar o solo a un miembro del grupo familiar.

Si solo se protege el registro de un miembro (es decir, un joven que participa en el Desarrollo de la Juventud y la Fuerza Laboral), los servicios que recibe aparecerán en la pantalla del Plan de Acción del Grupo Familiar. Los únicos datos protegidos son los datos en Detalles del Cliente.

¿Quién puede abrir el registro del cliente?

Si se utiliza la configuración de seguridad de inclusión, todo el personal podrá ver que el empleado tiene un Registro de Cliente en CMS, pero solo un grupo seleccionado podrá abrirlo. Los Administradores de la Agencia siempre tendrán acceso al Registro del Cliente. Si el cliente participa activamente en un Programa, los

Administradores de la Agencia determinarán con el personal del Programa quién necesita acceso al Registro del Cliente para proporcionar servicios. Como mínimo, sería el Trabajador del Caso y el Supervisor para ese Programa. El empleado de CAPV no tendrá acceso a su Registro de Cliente ni a los Registros de Cliente de los miembros de su hogar.

Si se utiliza la configuración de seguridad de exclusión, todos los empleados podrán ver y abrir el Registro del Cliente, excepto el empleado específico de CAPV identificado para excluir. En ese caso, ese empleado puede ver el registro, pero no puede abrirlo.

Un nuevo cliente se aplica a mi Programa y cuando busco en su registro, no puedo abrirlo. ¿Qué hago?

Esto puede suceder cuando un Cliente (ya sea un empleado de CAPV, un miembro de su grupo familiar o un cliente no empleado) que previamente obtuvo servicios de CAPV y optó por proteger sus datos busca un nuevo servicio. En este caso, póngase en contacto con los Administradores de la Agencia para añadir los empleados adecuados a la configuración de seguridad de inclusión. Los Administradores de la Agencia también se pondrán en contacto con el empleado de CAPV para notificarle que hay un cambio en su configuración para proporcionarles servicios. El personal del programa notificará al cliente no empleado que hay un cambio en la configuración de seguridad.