NNEDV

Prácticas recomendadas al utilizar el correo electrónico

Muchos programas de servicios para las víctimas utilizan a diario el correo electrónico en el trabajo, ya sea para comunicarse directamente con sobrevivientes o para coordinar servicios con otros programas comunitarios. Sin embargo, el correo electrónico es, por naturaleza, una forma de comunicarse que implica riesgos. Un correo electrónico puede reenviarse o ser leído por alguien a quien no estaba dirigido. Las siguientes son prácticas recomendadas para las agencias de servicios a la víctima que aseguran que su comunicación por correo electrónico se mantiene lo más privada y protegida posible.

Cuándo intercambiar correos electrónicos con los sobrevivientes

- No prohíba el intercambio de correos electrónicos con los/las sobrevivientes como una práctica general. Aunque los correos electrónicos implican riesgos, no permitir que los/las sobrevivientes utilicen el correo electrónico no es la solución. Permita que el/la sobreviviente determine los medios de comunicación que mejor se puedan adaptar a su capacidad, acceso, necesidades y preferencias.
- Si un/a sobreviviente lo/a contacta por correo electrónico, su respuesta:
    - No deberá contener el correo electrónico inicial y/o cualquier otro anterior. De esta forma, si el/la agresor/a intercepta o accede al correo electrónico, el pedido de ayuda o el historial de conversación completo no será revelado.
    - Deberá incluir información sobre los riesgos relacionados a la comunicación por correo electrónico (ejemplo a continuación) y analizar la seguridad y privacidad de los correos electrónicos con los/las sobrevivientes, para incentivarlos/las a eliminar los mensajes que hayan enviado y recibido y para vaciar la carpeta de elementos eliminados.
    - Deberá preguntar si existen maneras más seguras en las que pueda comunicarse. (Para algunos/as sobrevivientes, es posible que este sea el

único método disponible para obtener ayuda, pero para otros/as, una llamada telefónica o una visita en persona puede resultar más seguro).

  - Si la comunicación continúa, verifique periódicamente si el correo electrónico aún sigue siendo un método seguro y preferido de comunicación.

- No guarde los nombres y cuentas de correos electrónicos de las víctimas en una agenda.
- Si debe imprimir una conversación por correo electrónico, destrúyala en cuanto ya no la necesite.
- La mayoría de los programas terminarán de completar el resto de la dirección luego de que usted teclee las primeras letras del nombre. Para evitar enviar correos electrónicos a la persona equivocada, asegúrese de verificar dos veces la dirección antes de presionar enviar.
- El personal deberá eliminar regularmente los correos electrónicos de los/las sobrevivientes para no conservar información identificatoria y confidencial durante más tiempo del que sea necesario. Esto también incluye vaciar las carpetas de correos "enviados" y "eliminados".

Cuándo enviar correos electrónicos a los compañeros de trabajo sobre los sobrevivientes

- La comunicación interna sobre los/las sobrevivientes deberá estar restringida. Antes de enviar un correo electrónico a un/a compañero/a de trabajo sobre un/a sobreviviente, considere opciones que aumenten la privacidad, como hablar con el/la colega en persona o por teléfono.
- No incluya el nombre u otro tipo de información identificatoria de el/la sobreviviente en los correos electrónicos, incluidas las iniciales.

Cuándo enviar correos electrónicos a terceros externos sobre los sobrevivientes

Antes de utilizar el correo electrónico para comunicarse con terceros (incluso mediante un correo electrónico codificado), primero deberá determinar si existen otras opciones que se centren más en el/la sobreviviente y que no dejen un rastro

o huella digital. Abrir la puerta a la transmisión de información confidencial por correo electrónico es muy arriesgado. Antes de hacer eso, deberá asegurarse de que cada miembro del personal de su agencia que utilizará el correo electrónico para comunicar información confidencial de el/la cliente/a esté altamente capacitado/a sobre las obligaciones de confidencialidad de la Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés), la Ley Servicios y Prevención de Violencia Familiar (FVPSA, según sus siglas en inglés) y la Ley de Víctimas de Delito (VOCA, según sus siglas en inglés), y que entiende los riesgos y matices relacionados con la comunicación por correo electrónico. Cuando uno está atrapado en las idas y vueltas de una conversación por correo electrónico, es muy común olvidar o, accidentalmente, pasar por alto las limitaciones específicas que un/a sobreviviente ha establecido sobre el permiso que le otorgó para divulgar su información. Los/las intercesores/as pueden fácilmente compartir más de lo que se les ha permitido al responder preguntas de seguimiento.

Si usted decide continuar utilizando el correo electrónico, asegúrese de respetar las prácticas recomendadas que se detallan a continuación:

- Usted solo puede hablar sobre un/a sobreviviente con otra agencia por correo electrónico cuando el/la sobreviviente quiera que usted lo haga, y usted solo puede comunicar la información específica que lo/la hayan autorizado a compartir. Al hacer esto, usted debe tener un formulario de autorización escrita, informada y de tiempo limitado de parte de el/la sobreviviente antes de compartir cualquier información. Consulte lasHerramientas de confidencialidad de NNEDV Red Nacional para Eliminar la Violencia Doméstica para más información sobre obligaciones de divulgación y confidencialidad.
- Asegúrese de que todos/as los/las sobrevivientes estén bien informados/as sobre cómo se verá su información compartida por correo electrónico y los riesgos que esto implica, de modo que los/las sobrevivientes puedan tomar una decisión informada sobre la información que quieren compartir o no de esta manera.

Los/las intercesores/as deberán estar preparados para hablar sobre la manera en que su agencia está trabajando para asegurar que los correos electrónicos sean seguros y sobre cualquier riesgo potencial (por ejemplo: que usted no pueda controlar lo que la otra persona hace con el correo electrónico una vez que lo recibe; que tal vez deba enviarle a usted una respuesta en un documento codificado, etc.).

Correo electrónico seguro

Existen muchos productos en el mercado que afirman ofrecer correos electrónicos seguros y codificados. La mayoría de los/las proveedores/as de correos electrónicos (incluso muchos de ellos comercializados como codificados) tienen acceso al contenido de los correos electrónicos que los/las dueños/as de las cuentas envían y reciben. Si pueden acceder al contenido, entonces la comunicación no puede considerarse como verdaderamente confidencial. Para más información sobre requerimientos de confidencialidad para proveedores de servicios para víctimas de acuerdo con la ley federal, consulte nuestra Herramientas de confidencialidad.

Una protección más fuerte se conoce como "codificación de cero conocimiento", que hace que los datos enviados y recibidos sean ilegibles para la empresa de software que aloja el correo electrónico. Es importante saber que aunque este tipo de seguridad protege adecuadamente los datos de la víctima -mientras el programa espía (spyware) no esté en el dispositivo-, también complica el proceso de enviar y recibir correos electrónicos, así los miembros del personal y cualquier tercero externo tendrá que recibir capacitación sobre cómo utilizar tal software.

Prácticas y políticas recomendadas de las agencias

Las empresas deberían contar con una política de retención de datos que asegure que la información que no es necesaria se elimine regularmente. (Visite las herramientas de recursos de confidencialidad de NNEDV Red Nacional para Eliminar la Violencia Doméstica sobre prácticas recomendadas respecto de la retención y eliminación de registros). Esta política debería incluir los correos electrónicos enviados y recibidos de los/las sobrevivientes y los correos

electrónicos que contengan información sobre los/las sobrevivientes. No olvide que los correos electrónicos se guardan o archivan con frecuencia y las conversaciones por correo electrónico entre usted y los/las sobrevivientes se guardarán, por eso, también será necesario eliminar las copias de seguridad y los archivos que contengan información de los/las sobrevivientes.

Cuando se comunique con otros/as sobre los/las sobrevivientes, asegúrese de estar respetando las obligaciones de confidencialidad y los requisitos de privilegio de su organización (si su estado tiene un privilegio intercesor/a-cliente/a. El correo electrónico es una forma de registro escrito; protéjalo con responsabilidad.

Ejemplo de texto sobre exención de responsabilidad a incluir en el correo electrónico

Debido a que son pocas las personas que realmente leen la información en los renglones de firma, ser creativo al utilizar la cláusula de exención de responsabilidad podrá ayudar a que el mensaje llegue con mayor efectividad. El texto a continuación puede incluirse al comienzo de cada correo electrónico con un/a sobreviviente.

> Las comunicaciones entre [agency name] y los/las clientes/as están protegidas por el privilegio de [state, if applicable] y las leyes federales de confidencialidad. [Agency name] no revela o comparte comunicaciones de los/las clientes/as sin una autorización por escrito de el/la cliente/a, excepto cuando se le solicita hacerlo por disposición de informe obligatorio. Sin embargo, queremos asegurarnos de que usted es consciente de los riesgos de privacidad relacionados con la comunicación por correo electrónico:
>
> - Los correos electrónicos no son una forma segura para comunicarse.
> - Cualquier persona puede ver los correos electrónicos sin que usted lo sepa o sin su consentimiento. Por ese motivo, limite la información

personal identificable que envía en los correos electrónicos a solo lo que sea necesario.

- El personal de [agency name] puede conversar más con usted sobre las maneras de aumentar su privacidad y seguridad en línea.

 Financiado por la Oficina de Víctimas de Delitos del Departamento de Justicia (OVC, DOJ, por sus siglas en inglés) de Estados Unidos. Subvención n.º 2016-TA-AX-K064. Las opiniones, hallazgos, conclusiones o recomendaciones aquí expresados pertenecen a el/la autor/a y no necesariamente reflejan los puntos de vista del Departamento de Justicia (DOJ, por sus siglas en inglés).

Actualizamos nuestro material con frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.