Condiciones de cesión de la Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés), Privacidad de las Víctimas y Procedimientos de Supervisión Efectivos

Alicia Aiken, J.D.
Instituto de Confidencialidad

En esta herramienta práctica, la Parte I cubre las reglas para la protección de la privacidad y la información de las víctimas. La Parte II ofrece estrategias para llevar a cabo auditorías sobre dichas reglas. La Parte III ofrece estrategias de colaboración y recursos clave para brindar asistencia en casos de conflicto o incertidumbre.

Parte I
Las reglas

Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés):

"[L]os/las cesionarios/as y subcesionarios/as de [VAWA] no divulgarán, revelarán ni publicarán información personal identificable (PII, por sus siglas en inglés) recopilada en relación con los servicios solicitados, utilizados o denegados mediante los programas de cesionarios/as y subcesionarios/as, independientemente de que la información haya sido cifrada, encriptada, que contenga contraseña o esté protegida de otro modo[.] **34 USC §12291(b)(2)**

En gran medida, ese es el fin de la historia. Las condiciones de concesión de la Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés) exigen que los/las cesionarios/as "protejan la confidencialidad y privacidad" de las personas que reciben servicios de proveedores que reciben dicho financiamiento. Las dificultades para proteger de forma completa la información personal identificable suelen presentarse frente a tres circunstancias:

(1) Cuando los/las cesionarios/as creen que deben compartir información a pesar de lo establecido;

(2) Cuando los/las administradores/as del financiamiento creen que tienen derecho a acceder a la información a pesar de las reglas; y

(3) Cuando un/a aliado/a cree que se le puede confiar la información y buscan alternativas a la regla.

Para garantizar la privacidad apropiada de la víctima, los/las cesionarios/as, los/las administradores/as del financiamiento y los/las aliados/as deben aprender las reglas sobre las mejores prácticas y estar preparados/as para cumplirlas.

La privacidad implica respetar el derecho de una persona a tener el control de su información personal. Siempre que un programa esté considerando compartir, distribuir, manipular o divulgar de cualquier manera la información personalmente identificable, el programa deberá tener en cuenta el impacto sobre la privacidad. ¿Infringe la divulgación el control personal de las víctimas y sus familias sobre la información acerca de sí mismos/as? Para proteger su "confidencialidad y privacidad", las víctimas de violencia deberían decidir por sí mismos/as si su información personalmente identificable debería ser divulgada por un/a cesionario/a.

Para proteger adecuadamente la PII de las víctimas, los programas deben determinar qué se considera como "divulgación de información personalmente identificable". La Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés) define la información personalmente identificable de la siguiente manera:

> *"…información personal identificable de un individuo, o sobre él/ella, que incluye información que es probable que revele la localización de una víctima de violencia doméstica, violencia en las citas, agresión sexual o acecho, lo cual incluye la siguiente información:*

(A) nombre y apellido;
(B) domicilio particular u otra dirección física;
(C) información de contacto (incluido un correo postal, un correo electrónico o una dirección de protocolo Internet
, o un número de fax o de teléfono);
(D) un número de seguro social, número de licencia de conducir, número de
pasaporte o número de identificación de estudiante, y
(E) cualquier otra información, incluidas la fecha de nacimiento, origen étnico
o racial o afiliación religiosa que sirva para
identificar a un individuo".

- Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés) 2013, 34 USC §12291(a)(20)

Dada la manipulación de datos disponible a través de la tecnología moderna, casi cualquier conjunto de puntos de datos combinados vinculados a un individuo (incluso a alguien anónimo) se convierte en información potencialmente identificable.

Debido a que los/las agresores/as o atacantes pueden estar altamente motivados/as para buscar información sobre sus víctimas, los programas deberían revisar permanentemente las prácticas para asegurarse de que brindan protección contra esto. Los/las agresores/as pueden reclutar a otras personas para que los/las ayuden a ubicar y exponer a sus víctimas (*y, de hecho, lo hacen*) de forma que toda información que pudiera vincular a una víctima con un programa específico podría ser investigada como herramienta para acosar o rastrear a una persona. Pueden solicitar a familiares que trabajen con agencias estatales que accedan a bases de datos, convencer a oficiales de policía que trabajen como investigadores/as de informes de personas desaparecidas, o contratar investigadores/as privados/as bajo falsos pretextos.

Incluso cuando los programas envían informes desde sus bases de datos con información agregada sobre las víctimas (con la intención de que tales datos agregados le den anonimato a los individuos), los programas deberían considerar, en primer lugar, si tal información podría ser verificada mediante referencias cruzadas con otras bases de datos con información identificable (como una base de datos de HMIS o sitios Web de noticias).

A continuación se detallan algunas preguntas útiles que pueden hacerse cuando se considere si la privacidad de una víctima está o no en peligro:

1. "¿De qué manera puede utilizarse esta información para identificar, localizar o causar daños a la persona que me la confió?"
El daño emocional o de reputación es tan perjudicial como el daño físico en este análisis.

2. "¿Cuenta esto como divulgación?"
Si los/las cesionarios/as o subcesionarios/as ponen la información personalmente identificable en manos de cualquier persona fuera del programa de servicios para las víctimas (de forma literal o electrónica) o que pongan información en riesgo considerable de que se filtre del programa, entonces tienen un problema de divulgación. En el pasado, algunos/as patrocinadores locales e inclusos gubernamentales creían que podían recibir información personalmente identificable y confidencial siempre que estuviera encriptada para protegerla contra el *hackeo* u otro tipo de infiltración de datos. Sin embargo, el suministro de información personalmente identificable a los/as patrocinadores de forma encriptada *sigue* siendo una forma de divulgar información personalmente identificable a terceros/as; el patrocinador es un tercero. La encriptación solo previene que *otros/as* terceros/as accedan a tal información.
La transmisión de información confidencial sobre los/las sobrevivientes a los/as patrocinadores viola la privacidad individual porque pone la información fuera del control de la víctima. La divulgación aumenta el riesgo de que se filtre de forma más amplia, ya que la mayoría de los/as patrocinadores no cuentan con las mismas protecciones legales contra la divulgación forzosa como los/as

proveedores de servicios. Para algunos/as patrocinadores basados en el gobierno, cualquier información que reciban podría formar parte de sus "registros públicos" y estar sujeta a la divulgación a solicitud de cualquier persona o medio de comunicación. Otros patrocinadores podrían verse obligados/as a divulgar información de acuerdo con una citación ("subpoena") u otra acción legal, aun cuando los albergues para casos de violencia doméstica hayan tenido el privilegio de prevenir la divulgación.

Para proteger la seguridad de las víctimas, las agencias deberían desarrollar una política que establezca que la divulgación (mandato legal o consentimiento informado ausente) está prohibida, y deberían expresar con claridad que compartir información fuera del programa de servicios para víctimas (incluso con aliados/as y patrocinadores) se considera divulgación.

3. "¿Es ésta información identificable, incluso si se presenta en un informe agregado?"

Los programas pueden compartir habitualmente información personal no identificable con los/as patrocinadores y el público general. Al compartir datos agregados, los programas deben estar atentos a que no se convierta en información identificable. Si una familia o una persona en particular es demográficamente inusual en la comunidad (debido a su origen nacional, raza, tamaño del núcleo familiar, identidad de género, etc.), entonces la información de la persona no puede ser agregada de forma segura.

Imagine que un programa presta servicios a 100 sobrevivientes blancos/as, 100 sobrevivientes afroamericanos/as y un/a sobreviviente asiático/a. Divulgar esos números fuera del programa plantea un riesgo relativamente importante de que se pueda identificar a él/la sobreviviente asiático/a. Del mismo modo, la identificación de un cliente anónimo asiático de un programa como una persona embarazada, transgénero o padre/madre de seis niños/as aumenta el riesgo de reidentificación. Cualquier categoría demográfica que combine determinadas características y un grupo pequeño de individuos puede permitir la identificación.

Para preservar la privacidad de los/las sobrevivientes, los programas deberían emplear categorías amplias de informe, como "otros/as" para los servicios de captación ofrecidos en función de valores demográficos atípicos. Los programas igualmente pueden analizar tal información de forma interna para determinar si la persona es demográficamente excepcional *o* si el programa necesita intensificar el alcance a los/las sobrevivientes en tales grupos demográficos. Sin embargo, querrán evitar compartirlos fuera del programa de servicios para las víctimas.

Excepciones respecto de cuándo puede divulgarse información personalmente identificable

Teniendo presente la privacidad, los/las cesionarios/as pueden – y, algunas veces, deben – divulgar la información personalmente identificable en circunstancias muy acotadas. Estas situaciones se resumen a continuación.

1) La información generada por oficiales de policía, fiscales y la corte puede ser divulgada *por tales entidades*. Esta excepción no se aplica en el caso de cesionarios/as de proveedores de servicio a la víctima basados en comunidades, ya que no forman parte de agencias policiales, oficinas de fiscales ni cortes. Sin embargo, los/las cesionarios/as deben conocer esta excepción, y todos los sistemas asociados deberían asistir a los/las sobrevivientes a conectarse con los/as proveedores de servicios para víctimas que sean capaces de proteger por completo la información personalmente identificable cuando sea adecuado hacerlo.

2) Cuando un programa esté sujeto a una **orden válida de la corte** (por ej., una orden de allanamiento debidamente dictada), podrá divulgar la información identificada específicamente por la corte. Si una decisión de corte sienta un precedente a nivel estatal que exige la divulgación de determinada información (por ej., el deber consuetudinario de advertir), entonces los programas patrocinados por la ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés) pueden cumplir con tal deber. Tenga en cuenta que una citación ("subpoena") no es necesariamente lo mismo que una orden judicial final en la mayoría de las jurisdicciones y podría no implicar una excepción a las obligaciones

de confidencialidad. En situaciones en las que se emite una orden válida de la corte, los programas pueden divulgar la información solicitada, y también deberán:

a) hacer los intentos razonables para notificar a las víctimas afectadas por tal divulgación,
b) y adoptar las medidas necesarias para proteger la seguridad y la privacidad de las personas
afectadas por la divulgación de la información.

- Un paso fundamental para proteger la privacidad es contratar a un/a abogado/a para el programa o que el/la abogado/a ya empleado/a evite la ejecución de las citaciones u órdenes de la corte que violen la política pública o las leyes estatales. Los programas que deben afrontar la ejecución de una citación ("subpoena") pueden acceder a los siguientes recursos para recibir ayuda técnica:

    - Material de capacitación para abogados/as del Proyecto de defensa de citación ("subpoena") "Protecting Privacy to Enhance Safety" [Protección de la privacidad para mejorar la seguridad] de la Asociación Estadounidense de Abogados y el Instituto de Confidencialidad

    - Conjuntos de herramientas de confidencialidad y tecnología disponibles en techsafety.org/resources

    - Red de seguridad tecnológica en asociación con el Instituto de Confidencialidad disponible en safetynet@nnedv.org

3) Cuando un programa está sujeto a **mandato estatutario válido** se le permite divulgar la parte limitada de información personalmente identificable solicitada por tal mandato. Como se indicó anteriormente, también se le exige al programa que adopte medidas de protección y que haga los intentos razonables para notificar a la víctima.

- La divulgación debe ser realmente *exigida* y no simplemente *permitida*, y debe ser ordenada por un *estatuto*, no solo por una regulación, procedimiento o política gubernamental. Si un contrato de financiación estatal ordena a los/as receptores a compartir información identificable con agencias estatales, incluso si no existe una ley estatal que lo exija, entonces no se trata de un mandato estatutario y no crea una excepción en virtud de la ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés). Si una agencia estatal emite una norma que exige que los centros de crisis por violación divulguen información personalmente identificable, esto no constituye un mandato estatutario. Siempre que un programa experimente un exceso en la demanda de divulgación de información personalmente identificable, entonces tal programa tiene la obligación de poner un freno, hacer valer la norma de no divulgación de la ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés) y determinar si se aplica una excepción. Los programas pueden acceder a los mismos recursos detallados anteriormente para recibir asistencia para cumplir con los mandatos de la ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés).

Divulgaciones: ¡Mantente alerta con las medidas WITS [escrito (W), informado (I) y de duración específica (TS)]!

Los/las sobrevivientes pueden ordenar a los programas que divulguen información personalmente identificable completando un permiso específico informado, por escrito y de duración razonablemente limitada. Es fácil recordar las normas de divulgaciones si recuerda mantenerse alerta con las medidas WITS:

- Escrito
- Informado
- De duración limitada
- Las publicaciones WITS específicas y centradas en los/las sobrevivientes

protegerán los intereses de privacidad de las víctimas. Conceptualmente, las publicaciones son una extensión de las reglas de no divulgación y privacidad, no una excepción a ellas.

Cuando un/a sobreviviente desea que el programa divulgue información personalmente identificable de forma identificable, el/la sobreviviente ejerce su derecho a controlar su propia información. El programa simplemente actúa como agente del/de la sobreviviente respecto de la divulgación y no actúa por cuenta propia ni sirve sus propios intereses. Las publicaciones nunca deben ser exigirse ni se debería esperar que ocurran sistemáticamente. En virtud de la Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés), un/a cesionario/a no puede publicar información como condición para recibir servicios.

La práctica centrada en el sobreviviente implica que cada sobreviviente decidirá de qué manera la divulgación de la información personalmente identificable se adapta a sus objetivos individuales y a su plan de seguridad. Hay un formulario de publicación modelo disponible en el Conjunto de herramientas de confidencialidad de NNEDV Red nacional para Eliminar la Violencia Doméstica que se encuentra en techsafety.org/confidentiality-templates.

Condiciones del beneficio de la Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés), privacidad de las víctimas y procedimientos de supervisión efectivos

Alicia Aiken, J.D.
Instituto de Confidencialidad

En esta herramienta práctica, la Parte I cubre las reglas para la protección de la privacidad y la información de las víctimas. La Parte II ofrece estrategias para llevar a cabo auditorías sobre dichas reglas. La Parte III ofrece estrategias de colaboración y recursos clave para brindar asistencia en casos de conflicto o incertidumbre.

Parte II
Respetar las Reglas

Los programas, los/las administradores de subvenciones y los/las aliados/as pueden trabajar en conjunto para respetar las reglas de privacidad. Consideremos la pregunta más frecuentemente realizada que surge y las formas de resolverla, a la vez que protegemos la privacidad de las víctimas:

Llevar a cabo auditorías de cumplimiento y rendimiento

Los/las cesionarios/as y los/las auditores/as no deberían leer los archivos sin procesar (ya sea en papel o en formato electrónico) de un programa de servicios a las víctimas como parte de la gestión, supervisión o auditoría de subvenciones. Existen maneras alternativas para que los/las cesionarios/as y los/las auditores/as evalúen el cumplimiento y el rendimiento sin acceder a los archivos sin procesar que contienen información personalmente identificable de los/las sobrevivientes. El gobierno federal ha financiado durante mucho tiempo a profesionales de la confidencialidad, como abogados/as de servicios legales, y ha realizado auditorías de rutina apropiadas sin la necesidad de violar el privilegio cliente-abogado/a.

Deberían seguirse los mismos protocolos para los archivos de programas de servicios a las víctimas

Tanto el/la aduditor/a como el programa deben empezar por entender las reglas de confidencialidad del programa (ya sea que surjan de la ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés), la Ley de Servicios y Prevención de Violencia Familiar (FVPSA, por sus siglas en inglés) y la Ley de Víctimas de Delito (VOCA, por sus siglas en inglés), otras condiciones financieras, leyes estatales o mejor práctica basada en misión). Posteriormente los/las auditores/as deben identificar qué información es *realmente necesaria* para evaluar de manera efectiva el cumplimiento y el rendimiento. A continuación analicemos cómo confirmar la finalización del trabajo de forma adecuada sin divulgar información personalmente identificable. Aquí hay algunas estrategias prácticas que suelen funcionar:

- Un programa puede presentar números agregados de personas atendidas y servicios prestados *y* ofrecer una explicación detallada de su proceso aprobado por la junta para contar los/as clientes y servicios provistos.
- Juntos, el programa y el/la auditor/a pueden acordar una lista de verificación relacionada con cada cliente que no incluya información personalmente identificable pero que refleje la confirmación del programa respecto de los servicios que fueron prestados a cada cliente.
- Un/una auditor/a puede sentarse frente al Director Ejecutivo (o la persona designada) que tenga acceso a los archivos y hacerle preguntas de respuesta sí/no sobre el cumplimiento. Se le puede indicar al Director Ejecutivo que extraiga uno de cada cinco archivos de un cajón o uno de cada cinco nombres de una lista generada electrónicamente.
- Un programa puede entregar a todos/as sus clientes un código identificador de cliente (que no tenga ninguna relación con información personalmente identificable) para facilitar la creación de listas anónimas de

personas atendidas. La clave de tal código no saldrá del programa ni será compartida con el/la auditor/a.

- Un/a auditor/a puede solicitar acceso a archivos extraídos al azar con toda la información personalmente identificable eliminada. El/la auditor/a luego revisará los archivos copiados eliminados en el sitio del programa, y las versiones redactadas son trituradas cuando finaliza la auditoría.
    - La redacción es la opción que más recursos exige y con mayores probabilidades de violar requisitos de confidencialidad federales mediante la divulgación involuntaria de información personalmente identificable.
    - Los programas deben ser informados con anticipación sobre los archivos que se buscan a fin de asignar personal que dedique tiempo a eliminarlos.
    - Toda la información narrativa y demográfica debe ser leída y evaluada en función de su potencial de identificación, ya sea de manera directa o por contexto.
    - Un miembro del personal debe copiar los registros y eliminar la información personalmente identificable de forma permanente.
        - El marcador negro es a menudo insuficiente para eliminar la información personalmente identificable porque la tipografía aparece, especialmente cuando se hacen copias.
        - Los programas que utilicen la redacción deben considerar seriamente la posibilidad de comprar un producto, como Adobe Acrobat Pro, que eliminará de forma electrónica y permanente los datos seleccionados del documento, lo que permitirá que el programa publique la copia con la redacción sin correr el riesgo de divulgar información que fue eliminada.

        - Cubrir información de manera temporal con una nota adhesiva no constituye en una técnica de eliminación efectiva.

    - Otro miembro del personal debería leer los documentos con información eliminada para observar si la información restante, después de la redacción, puede ser utilizada para identificar a el/la sobreviviente o a miembros de su familia.

        - Por ejemplo, el/la autor/a de este documento recibió una vez un archivo con "información eliminada" de bienestar infantil en la cual se había suprimido el nombre de un testigo colateral, pero se había dejado una narración descriptiva del testigo como tío paterno del/de la menor, identificando de esta manera a la víctima.

    - Estos documentos se revisan en el sitio del proveedor y se destruyen una vez que la revisión del administrador/la auditoría haya finalizado.

Principales consideraciones respecto de las visitas al sitio en el cual los sobrevivientes reciben servicios

Las visitas al sitio que realizan los/las auditores/as en las ubicaciones donde los/las sobrevivientes reciben servicios (especialmente los albergues) siempre deben ser planificadas y nunca deben ser visitas sorpresa.

- La autonomía y el control de los/las sobrevivientes sobre la información es fundamental para proporcionar servicios efectivos relativos a la violencia familiar y doméstica.

- Para evitar que se repita el trauma, los programas deben preparar a los/las sobrevivientes para las visitas de auditores/as externos del gobierno y personal administrativo estatal.

- Los/las sobrevivientes pueden entonces escoger si prefieren estar en las instalaciones al momento de la visita o no.

- Mientras estén dentro del programa, no es apropiado que los/las administradores/as intenten ponerse en contacto con los/las sobrevivientes o que les pregunten sobre su experiencia.
    - Los programas pueden exhibir de manera prominente la información de contacto de el/la administrador/a de la subvención para cualquier sobreviviente que decida acercarse y compartir su experiencia con el/la proveedor/a de servicios a las víctimas.
- A pesar de tener las mejores intenciones, un/a auditor/a visitante puede quedar expuesto/a a información personalmente identificable sobre los/las sobrevivientes que reciben servicios, por lo cual todos/as los/las visitantes deben firmar un acuerdo de confidencialidad por adelantado que confirme que no divulgarán ningún tipo de información acerca de los/las sobrevivientes de los/as cuales tomen conocimiento durante la visita.

Exploraciones adicionales

A fin de continuar explorando otros métodos de supervisión sin violar la privacidad, los programas deberían consultar a los/las colegas que participen en los procesos de auditoría de otras profesiones confidenciales para averiguar de qué manera las llevan a cabo. Una advertencia: según su estado, los programas patrocinados por la Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés) pueden tener un nivel superior de protección de la privacidad que incluso abogados/as y médicos/as, por lo que nunca podrá saltarse el paso de comprender las normas que se aplican al programa específico que se auditará.

- La HIPAA permite compartir una parte bastante amplia de información de salud protegida con "asociados comerciales", siempre que el/la proveedor/a de atención sanitaria crea que es útil compartir información y que el/la asociado/a comercial acuerde contractualmente acatar las normas de el/la proveedor/a de atención sanitaria. Ni la Ley de Servicios y Prevención de Violencia Familiar (FVPSA, por sus siglas en inglés), ni la Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés) ni la Ley de

Víctimas de Delito (VOCA, por sus siglas en inglés) contienen excepciones para asociados/as comerciales.

Condiciones de cesión de la Ley de Violencia Contra las Mujeres (VAWA, por sus siglas en inglés), Privacidad de las Víctimas y Procedimientos de Supervisión Efectivos

Alicia Aiken, J.D.
Instituto de Confidencialidad

En esta herramienta práctica, la Parte I cubre las reglas para la protección de la privacidad y la información de las víctimas. La Parte II ofrece estrategias para llevar a cabo auditorías sobre dichas reglas. La Parte III ofrece estrategias de colaboración y recursos clave para brindar asistencia en casos de conflicto o incertidumbre.

Parte III
Colaboración, comunicaciones y asistencia técnica

De qué manera pueden colaborar los programas con asociados para atender a sobrevivientes

Los patrocinadores federales y no gubernamentales están poniendo cada vez más énfasis en la colaboración y la coordinación entre organizaciones y agencias. Estos son objetivos valiosos y los programas siempre deberían buscar maneras de colaborar que sean **consistentes con su misión y sus directrices**.

La "consistencia con la misión y las directrices" es el concepto clave. La privacidad de las víctimas y el control de su información es fundamental para el trabajo de los/as proveedores de servicios a las víctimas; por lo tanto, los programas de servicios a las víctimas no pueden hacer excepciones en cuanto a la divulgación para realizar colaboraciones con entidades externas.

Estas son algunas consideraciones referentes para cualquier proveedor/a de servicio a las víctimas que busque participar en la colaboración en la comunidad:

- Establezca un memorando de entendimiento que exponga lo siguiente:
    - Los objetivos de la colaboración, con un buen grado de especificidad cuantificable.
    - La identidad de cada participante/entidad que participan en la colaboración. Y
    - Las reglas de difusión de información (respecto de la divulgación y la no divulgación) aplicables a cada profesional/entidad en el grupo (como fiscales, oficiales de policía, proveedores de servicios a las víctimas, proveedores de atención sanitaria y educadores).

  Puede encontrar un modelo de memorando de entendimiento para socios/as colaboradores en el Conjunto de Herramientas de Confidencialidad de la NNEDV Red nacional para Eliminar la Violencia Doméstica en www.techsafety.org/confidentiality-templates.

- Considere enviar a un/a representante a la colaboración que no brinde servicios directamente y que no tenga conocimiento de información personalmente identificable para disminuir la probabilidad de divulgación de información personalmente identificable.

- Genere oportunidades para que los/as proveedores de servicios a las víctimas enseñen a otros/as participantes en la colaboración acerca de su trabajo, su misión y sus reglas. Las obligaciones de confidencialidad de los/as proveedores comunitarios/as de servicios a las víctimas pueden ser las menos conocidas dentro del equipo multidisciplinario, y la educación sobre la confidencialidad puede reducir significativamente la presión en los/las intercesores/as en cuanto a la divulgación. También puede ayudar a otras profesiones a comprender los parámetros de la información que los/as proveedores de servicios a las víctimas pueden ofrecer al esfuerzo de colaboración.

- Prepárese para las reuniones y hable con los/as clientes individuales sobre cómo pueden querer participar en la colaboración. Un/a cliente puede dirigir un/a intercesor/a para que actúe como agente y revele información específica. Los/as clientes no suelen pedirlo porque no se dan cuenta de que es posible; los/las intercesores/as tal vez deseen aumentar la conciencia de los/las sobrevivientes sobre esta estrategia para participar en las colaboraciones. Si un/a cliente quiere confiar en un/a intercesor/a como agente para revelar información, es necesario completar y seguir estrictamente un permiso de publicación escrito, informado y de duración razonable.

- Utilice preguntas sobre un/a sobreviviente individual como una oportunidad para hacer una intercesoría a nivel de sistemas sobre las necesidades de los/las sobrevivientes como grupo. Si un/a fiscal pregunta "¿tuvo relaciones sexuales con él antes de la presunta violación?", el/la intercesor/a puede responder: “La experiencia nos dice que las víctimas se sienten avergonzadas y culpadas por la violación cuando se investigan sus historias sexuales personales. Hacer una pregunta como esa podría ocasionar que un/a sobreviviente deje de cooperar con la fiscalía. ¿Puede ayudarme a entender por qué quiere saber esa información? ¿Qué impacto tiene la respuesta sobre si se hará un procesamiento o si se obtendrá una condena?” Este debate refuerza la colaboración, puede revelar información necesaria para el/la sobreviviente, y protege la información privada que conserva el/la intercesor/a sobre el/la sobreviviente.

Demostrar resultados

En este entorno de financiación cada vez más competitivo e impulsado por la información, los programas y las comunidades preguntan: “¿Cómo comunicamos las historias de éxito y explicamos nuestros resultados?”

Cuando un/a sobreviviente destaca a un centro de crisis por violación como la clave de su recuperación, genera un gran impacto en la comprensión pública del

valor de los servicios a las víctimas. Sin embargo, cuando un centro de crisis por violación decide utilizar la historia de un/a sobreviviente para promover objetivos de publicidad y recaudación de fondos definidos por el programa, corre el grave riesgo de violar la privacidad y de despersonalizar a el/la sobreviviente. Los programas tienen que pensar cuidadosamente sobre cuándo y cómo conseguir el permiso para usar la historia de una persona, ya que tienen gran parte del poder en la relación con el/la sobreviviente. A continuación se detallan algunas ideas sobre la forma de celebrar el éxito en consonancia con la protección de la privacidad de las víctimas y la misión de los servicios de atención a las víctimas:

- La participación en la medición de los resultados a largo plazo siempre debe ser totalmente voluntaria. Nunca sugiera a los/as clientes que la participación es habitual o que se espera que participen. No le pida a el/la sobreviviente que tome la decisión mientras habla con usted; ofrézcale tiempo y espacio para que lo considere con más detenimiento. Esté preparado/a para informar a el/la cliente sobre los beneficios que obtendrán de la participación. Los/as clientes tienen derecho a tener tiempo y privacidad para decidir si desean participar en los resultados cuantificables.

- Informe sus resultados como información agregada no identificable personalmente, no como información individual.

- Solicite la opinión de los/as clientes por diversos motivos; no simplemente para presumir sobre ellos en una publicidad o para realizar un seguimiento. Crear una atmósfera en la que los/as antiguos/as clientes sean bienvenidos/as a participar en la promoción de sistemas, la mejora de la calidad del programa y las oportunidades de voluntariado. Si un/a cliente decide que el camino de víctima a sobreviviente implica compartir públicamente los beneficios obtenidos, entonces colabore y deje que el/la cliente se encargue de contar su propia historia.

Cumplimiento con los requisitos de confidencialidad federales

La privacidad es extraordinariamente importante en esta labor, y la presión que ejerce el siglo XIX en la divulgación puede ser intensa, por lo cual los programas deberían obtener ayuda para asegurarse de permanecen dentro de los límites de los requisitos de confidencialidad federales.

Los programas y los/as administradores/as de subvenciones deberían debatir políticas y procedimientos de confidencialidad para ayudar a los/las beneficiarios/as a documentar el cumplimiento de las disposiciones relativas a la privacidad y la confidencialidad. Este proceso de "evaluación y garantías" puede detectar la necesidad de un cambio de procedimiento o de nuevas políticas. Y, si bien las reglas para la privacidad son lo suficientemente directas, la mejor manera de atenerse a ellas no es siempre obvia. A veces debemos soportar la carga de prácticas pasadas que violan la privacidad de las víctimas y cambiarlas puede parecer difícil o incluso imposible. Cuando los/as patrocinadores/as y aliados/as estén acostumbrados/as a cierto acceso a la información, el programa tendrá que abordar directamente el motivo por el cual se está produciendo el cambio, y garantizar que no se trata de una sentencia sobre la fiabilidad de un/a socio/a comunitario/a en particular.

Sin embargo, la protección de la privacidad de los/as supervivientes no es opcional. La falta de protección de la confidencialidad podría dar lugar a la pérdida de fuentes de financiación, la desconfianza de la comunidad de supervivientes e incluso una responsabilidad jurídica si el daño es ocasionado a partir de la divulgación no autorizada de información personalmente identificable.

Los/as administradores/as de subvenciones, las coaliciones y los programas individuales pueden obtener ayuda para implementar la confidencialidad correctamente:

- El Instituto de Confidencialidad (www.confidentialityinstitute.org) brinda capacitación nacional sobre privacidad, así como también asistencia técnica individual para resolver problemas de confidencialidad complejos.

- La Red Nacional para Eliminar la Violencia Doméstica es un proveedor de asistencia técnica nacional sobre la confidencialidad de sobrevivientes y trabaja estrechamente con el Instituto de Confidencialidad. Juntos han creado una conjunto de herramientas en línea con modelos, preguntas frecuentes, folletos con consejos y extractos de la ley. Puede encontrar el Conjunto de Herramientas de Confidencialidad en www.techsafety.org/confidentiality y puede enviar sus preguntas para asistencia técnica a safetynet@nnedv.org.

Financiado por Subvención N.° 2019-TA-AX-K003 otorgada por la Oficina de Violencia contra las Mujeres, Departamento de Justicia de los Estados Unidos. Las opiniones, hallazgos, conclusiones y recomendaciones expresadas en esta publicación/programa/exposición pertenecen a el/la autor/a y no reflejan necesariamente las opiniones del Departamento de Justicia, Oficina de Violencia contra las Mujeres.

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