HEARTLAND ALLIANCE INTERNATIONAL

Heartland Alliance International
Manual de privacidad y seguridad de la información
Colombia

Contenido

INTRODUCCIÓN

Aviso: Se espera que todos los miembros del personal de Heartland Alliance International (HAI) lean este manual en su totalidad y las cláusulas mencionadas en el manual de HA.

El tema de la ciberseguridad y la violación de Información Confidencial es uno de los mayores desafíos que enfrenta la comunidad global en el siglo 21. En una era digital, ningún individuo, organización o gobierno está a salvo de las tecnologías avanzadas utilizadas para infligir daños físicos, psicológicos, sociales o financieros.

El desarrollo internacional y el sector humanitario no son una excepción a esta mayor vulnerabilidad. El principio de *"no hacer daño"* mantiene al sector humanitario en un estándar ético más alto que otras industrias, dado su compromiso con el bienestar de la población vulnerable. En la última década, las principales organizaciones internacionales han expresado reiteradamente su preocupación por la falta general de conciencia sobre la privacidad y la seguridad de los datos en el sector de desarrollo internacional y humanitario. Los donantes gubernamentales y privados exigen cada vez más un conjunto de políticas sobre prácticas de datos y seguridad de la información. La introducción del manual de privacidad y seguridad de la información es, en parte, una respuesta a esta solicitud de cambio por parte de donantes y líderes del sector.

Al igual que muchos de sus pares, Heartland Alliance International (HAI) opera en lugares en todo el mundo que se están recuperando de una historia de conflictos, discriminación, opresión, bajos recursos y falta de infraestructura en el país. Estos factores preexistentes aumentan el riesgo de daños graves que enfrentan las personas cuando son víctimas de daños y explotación cuando se produce una violación de la información personal. A pesar del mayor riesgo de daños físicos, psicológicos, sociales y financieros graves, estas personas a menudo tienen menos recursos para evitar violaciones y mitigar las consecuencias.

La misión central de HAI es garantizar la seguridad y aumentar la sensación de seguridad de las personas que son sobrevivientes de violaciones graves de los derechos humanos. Por lo tanto, la operación de HAI debe alinearse con priorizar la seguridad personal, ya sea física, psicológica, social o financiera, de sus participantes y otras personas involucradas en la implementación de su programa.

Con el fin de proteger a sus participantes, miembros de la fuerza laboral y afiliados, HAI está lanzando su propio manual adaptado al contexto operativo por fuera de los Estados Unidos.

El Capítulo 1 analiza el conjunto de principios que justifican el desarrollo de políticas específicas de HAI y la necesidad de una mayor protección de la información personal. El primer principio es uno de los principios más antiguos y fundamentales del humanitarismo, el principio humanitario de "no hacer daño". Los principales actores del sector humanitario expresan su preocupación por las amenazas contra la privacidad y la seguridad de la información más que nunca. Esto llega en un momento en que el mundo está siendo testigo de un creciente número de ataques cibernéticos por parte de piratas informáticos y regímenes opresivos, y el reciente alboroto sobre el uso de tácticas invasivas por parte de las empresas de redes sociales para recopilar, almacenar y vender datos personales a entidades con agenda comercial y política. Los principales donantes del sector humanitario, tales como organizaciones internacionales, gobiernos, fundaciones e individuos, exigen cada vez más medidas de protección como condición para la financiación. Garantizar la privacidad y la seguridad de la información ha pasado de ser un gesto de buena voluntad a una cuestión de cumplimiento con los requisitos legales y de los donantes.

El Capítulo 2 proporciona la definición de Información Confidencial, la política de HAI sobre Información Confidencial, detalles sobre usos aceptables de información privada y/o confidencial durante la operación de HAI, y la responsabilidad de los miembros de la fuerza laboral y afiliados de HAI de realizar la debida diligencia para proteger de violaciones cualquier información de naturaleza confidencial que puedan encontrarse durante la operación de HAI.

El Capítulo 3 proporciona protocolos sobre el procesamiento de información que tiene lugar todos los días en HAI. Los miembros de la fuerza laboral y afiliados de HAI interactúan con información de diferentes niveles de sensibilidad. Este documento llamará a esta interacción *el 'procesamiento'.* Este capítulo proporcionará un conjunto de protocolos

de protección para cada etapa del procesamiento de datos: recopilación de información/recopilación de datos, información control de acceso/almacenamiento, y protocolo de intercambio de información.

Capítulo 4 incluye información y protocolos de ciberseguridad.

El Capítulo 5 discute lo que constituye un 'incidente de incumplimiento' y proporciona una descripción del plan de respuesta. Los incidentes de incumplimiento inevitablemente socavarán la confianza entre HAI y sus participantes, donantes, organizaciones asociadas y partes interesadas locales.

El Capítulo 6 proporciona un resumen de las leyes locales de privacidad que las oficinas de país de HAI deben cumplir. Los lectores pueden consultar la lista exhaustiva de requisitos de privacidad de cada país donde HAI se encentra operando. Antes del comienzo de nuevos negocios en cualquier país nuevo, el Gerente de Seguridad de HAI debe ser notificado para recibir orientación sobre el desarrollo de políticas y leyes estatales aplicables.

Para preguntas relacionadas con este manual u otras preocupaciones de privacidad o seguridad, puede comunicarse con Eryn Yaejung Lee (elee@heartlandlliance.org), Gestión de Riesgos Empresariales por correo electrónico a ERM@heartlandalliance.org o puede comunicarse con el Gerente de Seguridad Internacional de Heartland Alliance que se indica a continuación, Noah Lane (nlane@heartlandalliance.org) .

REFERENCIA A LA POLÍTICA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN DE HEARTLAND ALLIANCE

Como empresa, Heartland Alliance sigue una política de seguridad de la información descrita en el Manual de Privacidad y Seguridad de la Información de Heartland Alliance. El manual fue desarrollado para cumplir con las regulaciones legales en los Estados Unidos que protegen la privacidad y la información de salud de los participantes. Todas las entidades de Heartland Alliance ubicadas en los Estados Unidos deben cumplir con estos requisitos legales a nivel federal, estatal y local. Si bien las mejores prácticas para proteger la privacidad de los participantes y la seguridad de la información son globales, las oficinas de Heartland Alliance International fuera de los Estados Unidos deben cumplir con diferentes requisitos legales.

Este manual documenta las políticas de privacidad y seguridad de la información para los programas de HAI que operan por fuera de los Estados Unidos. Este documento, que aplica a cualquier operación de HAI en entornos no estadounidenses, describe las leyes de privacidad en los países donde opera HAI y brinda orientación sobre cómo proteger la Información Confidencial utilizando las mejores prácticas internacionales.

Este manual, creado en referencia al Manual de privacidad y seguridad de la información de Heartland Alliance (HA), consta de lo siguiente:

- Una versión modificada del manual de HA que aplica a la operación de HAI; los cambios fueron:

    a. eliminación de referencias jurídicas o políticas específicas a los Estados Unidos;
    b. cambio del nombre de la entidad de 'Heartland Alliance' a 'Heartland Alliance International;
    c. reemplazo de términos legales específicos de los Estados Unidos con términos y definiciones utilizados en el sector humanitario;
    d. inserción de normas de la Norma General de Protección de Datos 2016/679 (GDPR);
    e. incorporación de las mejores prácticas de protección de datos presentadas en el estándar Esfera, directrices del Comité Permanente Interagencial (IASC), grupo de trabajo de protección de InterAction y Comité Internacional de la Cruz Roja (CICR);

- Requisitos de los donantes de HAI sobre privacidad y seguridad de la información;

- Requisitos legales, incluidas las leyes de privacidad, de los países donde opera HAI;

- Seguridad operacional & evaluación de riesgos de seguridad de la información de cada país donde HAI se encuentra operando;

- La tabla de secciones en el manual de HA, la cual no requirió ninguna modificación. (Nota: solo los empleados de HAI pueden ver el texto completo; los enlaces web incrustados en los textos conectarán al lector a la Intranet).

Para el resto de este documento, el cuerpo colectivo de protocolos y directrices sobre privacidad y seguridad de la información que se aplica a las operaciones de HAI en entornos no estadounidenses se denominará "*Política de HAI*".

Los miembros de la fuerza laboral de HAI pueden acceder al texto completo del Manual de privacidad y seguridad de la información de Heartland Alliance ("Manual de HA") a través de la intranet. Si no es miembro de la fuerza laboral de HAI pero desea ver el texto completo del manual de HA como referencia, por favor solicite una copia de la sección correspondiente al personal de HAI.

GLOSARIO DE TÉRMINOS

El siguiente glosario de términos se utilizará en la política de privacidad y seguridad de la información de Heartland Alliance International (HAI). La siguiente terminología establece un lenguaje común para las discusiones sobre los protocolos de seguridad de la información dentro de la operación de HAI, pero los lectores deben tener en cuenta que las definiciones legales pueden variar según el país.

A

Acceso - significa cualquier acción que implique interacción con alguna información. En el contexto de la Información Confidencial, puede incluir las siguientes acciones:

a) escuchar, leer o entrar en contacto con Información Confidencial;
b) recopilar Información Confidencial de forma verbal o escrita (tanto electrónica como en papel);
c) *crear o copiar contenido que contenga Información Confidencial. 'Contenido' puede incluir, pero no está* limitado a:
- *archivos electrónicos*: documentos de Word, hojas de cálculo de Excel, diapositivas de PowerPoint, archivos de mensajes de correo electrónico, etc.
- *documentos físicos*: notas escritas a mano, documentos impresos, copias en papel del documento original, post-its, etc.
- *medios: archivos de audio, fotografías (tanto electrónicas como impresas), archivos de video, etc.*

d) almacenar contenido que contenga Información Confidencial en forma física (por ejemplo, medio de almacenamiento, cajón, cajuela de un vehículo, etc.) y/o realizar la configuración en línea (por ejemplo, de base de datos, unidad compartida, dispositivo móvil, etc.);
e) compartir o divulgar contenido que incluya Información Confidencial a cualquier persona o entidad.

Informe de Divulgación - Un documento que se mantiene para cada participante, el cual registra qué Información Confidencial fue utilizada/compartida/ revelada a quién por parte de HAI.

Afiliados - Una persona u organización, que no es miembro de la fuerza laboral, que realiza una función o actividad en nombre de HAI que involucra el uso o divulgación de Información Confidencial: información personal, información confidencial protegida (ICP)e información privilegiada. Un afiliado también puede ser una persona o entidad que proporciona servicios legales, actuariales, contables, de consultoría, de agregación de datos, de gestión, administrativos, de acreditación o financieros que impliquen el uso o divulgación de Información Confidencial. Afiliados incluye:

- Personal de medio tiempo y tiempo completo, consultor, asesor y voluntario de la organización sub-receptora de recursos;
- Cualquier persona que trabaje para entidades externas (p. ej., centro comunitario, centro médico, agencias gubernamentales) que desempeñe funciones centrales para o que apoyen las actividades del proyecto del programa de HAI.

Modificar/Enmienda - Una enmienda a la Información Confidencial siempre será en forma de información agregada a la Información Confidencial existente. Esta información adicional puede contener elementos que cambian sustancialmente la Información Confidencial inicial, hacen que partes de la Información Confidencial sean más

precisas o evidencian que parte de la Información Confidencial original es incorrecta. La Información Confidencial original nunca se modifica; los cambios se indican mediante la adición de la información modificada.

Anonimato - (usado indistintamente con 'desidentificación') El anonimato es el proceso utilizado para evitar que la identidad de una persona natural se conecte con alguna información. Para que una información sea anonimizada, debe haber una base razonable para creer que la información es lo suficientemente general como para que no pueda utilizarse para identificar a una persona.

Autorización - (usado indistintamente con 'consentimiento informado') Declaración de acuerdo del participante para el uso o divulgación de Información Confidencial —datos personales, información privada confidencial (ICP) o información privilegiada— a terceros.

B

Información biométrica - El procesamiento de las características biológicas o comportamentales de una persona, tales como imágenes faciales o huellas digitales, nos llevará a una única persona. La información utilizada en este proceso que identifica a una persona se denomina, en conjunto, biometría.

Violación - La adquisición, acceso, uso o divulgación de Información Confidencial de una manera no permitida por la política de privacidad y seguridad de la información de HAI, que compromete datos personales, información confidencial personal (ICP) o información privilegiada. Una violación excluye:

1. La adquisición, acceso o uso involuntario de datos personales o ICP por parte de un miembro de la fuerza laboral o afiliado que actúe bajo la autoridad de un proveedor de atención médica o socio comercial si se realizó de buena fe y dentro del alcance de la autoridad y no resulte en un uso o divulgación posterior;
2. La divulgación involuntaria por parte de una persona autorizada para acceder a datos personales o ICP en una entidad cubierta a otra persona autorizada a acceder a datos personales o ICP bajo el mismo arreglo con la organización o institución de atención médica en el que participa el proveedor de atención médica, y la información recibida no es utilizada ni divulgada.
3. Una divulgación de datos personales o ICP donde un proveedor de atención médica o socio comercial cree de buena fe que una persona no autorizada a la que se realizó la divulgación no habría podido retener dicha información de manera razonable

C

Información Confidencial - en conjunto, significa datos personales o Información Personal, información confidencial personal (ICP) e información privilegiada.

- *Información Personal*[1] significa cualquier información relacionada con una persona física identificada o identificable (el 'interesado'). Esto incluye todos los identificadores incluidos en la información de identificación personal (IIP). El término de Información Personal, para efectos de este Manual, es equivalente al de "Datos Personales", según lo define la Ley 1581 de 2012 y demás normativa aplicable en Colombia.

  Se puede identificar a una persona física en referencia a un identificador como un nombre, un número de identificación, datos de ubicación y un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona natural. *Ir a Información personal para una definición más detallada y ejemplos de identificadores.*

- *Información Confidencial Personal (ICP)* se refiere a información que es privada y que podría afectar a un individuo si se hace pública. Es importante recordar que un dato no tiene que ser necesariamente cierto para causarle un gran daño a una persona; el vínculo percibido entre la ICP y una persona es todo lo que necesitan aquellos que buscan hacer daño. El nivel de riesgo que un dato de ICP representaría para las personas varía en gran medida según su ubicación física y posición socioeconómica en la comunidad. Por lo tanto, la

[1] HAI utilizará la definición de datos personales de la GDPR (Fuente: GDPR, OJ L 241, 17.9). Los 'datos personales' indicados en este manual son más amplios que, y por lo tanto, incluyen la, información de identificación personal (IIP).

sensibilidad de los datos y las salvaguardas apropiadas deben considerarse caso por caso.). El término de Información Confidencial Personal, para efectos de este Manual, es equivalente al de "Datos Sensibles", según lo define la Ley 1581 de 2012 y demás normativa aplicable en Colombia. *Ir a Información Confidencial Personal (ICP) para una definición más detallada y ejemplos de identificadores.*

- *Información Privilegiada* incluye, pero no se limita a, información no pública que puede incluir planes de negocios, acuerdos, contratos, información financiera y de empleados, estrategias y técnicas. Los ejemplos de información no pública incluyen registros de personal, información bancaria y de registro y estrategias organizativas o detalles operativos que pueden afectar negativamente la ventaja competitiva de la organización.

Consentimiento[2] - (queriendo decir consentimiento informado) del interesado, significa cualquier indicación libremente dada, específica, informada y sin ambigüedades de los deseos del interesado por el cual él o ella, mediante una declaración o por una acción afirmativa clara, indica estar de acuerdo con el procesamiento de datos personales en relación con él o ella.

D

Interesado - significa cualquier persona (es decir, un individuo) cuyos datos personales se recopilan, retienen o procesan. El término de Interesado, para efectos de este Manual, es equivalente al de "Titular", según lo define la Ley 1581 de 2012 y demás normativa aplicable en Colombia.

Desidentificación - (usado indistintamente con 'anonimato') La desidentificación es el proceso utilizado para evitar que la identidad de una persona natural se conecte con alguna información. Para que una información sea anonimizada, debe haber una base razonable para creer que la información no puede utilizarse para identificar a una persona.

Conjunto de registros designado - Registros médicos, de facturación y de inscripción mantenidos y utilizados por HAI para tomar decisiones sobre el participante. Para fines de esta definición, un registro es cualquier elemento, recopilación o agrupación de información que contiene datos personales o información confidencial personal (ICP) y que es mantenida, recopilada, utilizada o divulgada por un centro de HAI.

Divulgación - La divulgación, transferencia, provisión, acceso o revelación de cualquier otra forma de información hacia afuera de la entidad que posee dicha información.

E

Escuchas - Cuando una persona a sabiendas e intencionalmente 1) utiliza un dispositivo de escucha, de manera subrepticia, con el propósito de escuchar, transmitir o grabar toda o parte de cualquier conversación privada de la cual él o ella no sea parte, a menos que él o ella lo haga con el consentimiento de todas las partes en la conversación privada; 2) utiliza un dispositivo de escucha, de manera subrepticia, con el propósito de transmitir o grabar toda o parte de cualquier conversación privada en la que él o ella sea parte, a menos que lo haga con el consentimiento de todas las otras partes de la conversación privada; 3) intercepta, registra o transcribe, de manera subrepticia, cualquier comunicación electrónica privada de la que no sea parte, a menos que lo haga con el consentimiento de todas las partes de la comunicación electrónica privada; 4) fabrica, ensambla, distribuye o posee cualquier dispositivo electrónico, mecánico, de espionaje u otro dispositivo sabiendo que o teniendo razones para saber que el diseño del dispositivo lo hace principalmente útil para escuchar, transmitir o registrar subrepticiamente las conversaciones privadas o realizar la interceptación o la transcripción de la interceptación electrónica privada, o la transcripción de la comunicación electrónica privada, y el uso previsto o real del dispositivo es contrario a lo dispuesto por la ley; o 5)

[2] Fuente: GDPR, OJ L 241, 17.9

usa o divulga cualquier información que él o ella sepa o que razonablemente deba saber que se obtuvo de una conversación privada o comunicación electrónica privada en violación de la ley, a menos que lo haga con el consentimiento de todas las partes. Fuente: 720 ILCS 5/14-2

Medios electrónicos - Material de almacenamiento electrónico en el que los datos se registran o pueden registrarse electrónicamente y los medios de transmisión se utilizan para intercambiar información que ya está en medios de almacenamiento electrónico.

Cifrado - El uso de un proceso algorítmico para transformar datos de manera que haya una baja probabilidad de asignarles significado sin el uso de un proceso o clave confidencial.

F

Instalaciones –Las instalaciones físicas y el interior y exterior de un edificio arrendado o de propiedad de HAI o sus socios comerciales en los que se pueda usar, almacenar, procesar y compartir Información Confidencial.

Familiar - Quiere decir, con respecto a un individuo; un dependiente del individuo; u otra persona que sea pariente de primer grado, segundo grado, tercer grado o cuarto grado del individuo o de un dependiente del individuo.

1. Los parientes de primer grado incluyen padres, cónyuges, hermanos e hijos.
2. Los parientes de segundo grado incluyen abuelos, nietos, tías, tíos, sobrinos y sobrinas.
3. Los parientes de tercer grado incluyen bisabuelos, bisnietos, tías abuelas, tíos abuelos y primos hermanos.
4. Los parientes de cuarto grado incluyen tatarabuelos, tataranietos e hijos de primos hermanos.

Sistema de archivado - significa cualquier conjunto estructurado de datos personales a los que se pueda acceder de acuerdo con criterios específicos, ya sean centralizados, descentralizados o dispersos de forma funcional o geográfica. Fuente: GDPR, OJ L 241, 17.9

G

Datos genéticos - quiere decir los datos personales relacionados con las características genéticas heredadas o adquiridas de una persona que brindan información única sobre la fisiología o la salud de esa persona natural y que resultan, en particular, del análisis de una muestra biológica de la persona física en cuestión. Fuente: GDPR, OJ L 241, 17.9

H

Cuidado de la salud - es la atención, servicios o suministros relacionados con la salud de un individuo, incluidos 1) cuidados preventivos, diagnósticos, terapéuticos, de rehabilitación, de mantenimiento o paliativos, y asesoramiento, servicio, evaluación o protocolo con respecto a la condición física o mental, o el estado funcional, de un individuo, que afecta la estructura o función del cuerpo; y 2) la venta o dispensación de un medicamento, dispositivo, equipo u otro artículo de acuerdo con una fórmula médica.

Operaciones de atención médica –Cualquiera de las siguientes actividades: realizar evaluaciones de calidad y actividades de mejora, actividades de seguridad del paciente, actividades basadas en la población, gestión de casos y coordinación de la atención, contactar a los proveedores de atención médica y al paciente con información sobre alternativas de tratamiento médico, revisar la competencia o las calificaciones de los profesionales médicos, evaluación del desempeño del proveedor, desempeño del plan de salud, realización de programas de capacitación, revisión médica, detección de fraude y abuso y programas de cumplimiento, planificación y desarrollo de negocios.

Proveedor de atención en salud –Un proveedor de servicios médicos o de salud y cualquier otra persona u organización cuya función principal de trabajo sea procesar la prestación y el pago de atención médica.

Datos de salud se refiere a los datos personales relacionados con la salud física o mental actual o pasada de una persona física, incluida la prestación de servicios de atención médica, que revelan información sobre su estado de

salud. Los datos de salud son parte de la información confidencial personal (ICP), que es privada y puede dañar a un individuo si se hace pública.

I

Incidente de seguridad de la información - Intento o éxito de acceso no autorizado, uso, divulgación, modificación o destrucción de información o interferencia con las operaciones del sistema en un sistema informático.

Sistema informático - Un conjunto interconectado de recursos de información bajo el mismo control de gestión directo que comparte una funcionalidad común. Un sistema normalmente incluye hardware, software, información, datos, aplicaciones, comunicaciones y personas.

Integridad - (en relación con TI) es la garantía de que la información es confiable y precisa y que no ha sido alterada o destruida de manera no autorizada.

TI - significa tecnología de la información.

L

Notas legales - notas registradas (en cualquier medio) por un proveedor de servicios legales: este puede ser un profesional del derecho con licencia para representar a personas, funcionarios legales, asistentes legales/auxiliares jurídicos o trabajadores sociales que están documentando información relevante a una cuestión legal. La documentación durante las consultas de carácter legal se considera privada y debe almacenarse en un lugar seguro que sea independiente del resto del archivo del caso del individuo.

M

Software malicioso - software o aplicación informática diseñada para dañar o interrumpir un sistema, es decir, un virus, spyware, malware, etc.

Marketing - Cualquier comunicación sobre un producto o servicio que aliente al destinatario a comprar o usar el producto o servicio; siempre, sin embargo, que los siguientes tipos de comunicaciones no sean considerados como "Marketing" en virtud de la prestación de atención en salud en la acción humanitaria, a pesar de que de otra manera podrían entrar en la definición general de "Marketing":

- Comunicaciones que describen un producto o servicio relacionado con la salud que es proporcionado por o incluido en un plan de salud o plan de beneficios suministrado por proveedores locales de atención médica;
- Comunicaciones sobre el tratamiento médico del individuo;
- Comunicación para la gestión de caso o la coordinación de atención para la persona o para dirigir o recomendar tratamientos médicos alternativos, terapias, proveedores de atención médica o entornos de cuidado para el individuo.

Notas de la sesión de salud mental y apoyo psicosocial (SSMAP) - notas registradas (en cualquier medio) por un proveedor de servicios de salud mental y apoyo psicosocial; este puede ser un profesional de salud mental con licencia, un trabajador social capacitado para proporcionar actividades de apoyo psicosocial (APS) o un funcionario de APS. Documentar o analizar el contenido de la conversación durante una sesión de asesoramiento privado o una sesión de asesoramiento grupal, conjunta o familiar, y mantenerlo separado del resto de la historia clínica del individuo.

O

Pruebas optativas - Un enfoque en el que se presenta una prueba de VIH ofreciendo la prueba y el paciente acepta o rechaza la prueba.

Pruebas de exclusión - Un enfoque en el que se presenta una prueba de VIH de modo que se notifique al paciente que pueden realizarse pruebas de VIH a menos que el paciente lo rechace.

P

Registro de participante es la recopilación de información sobre los servicios de los participantes que se crean o mantienen durante la operación normal. El Registro del participante incluye actos, eventos, diagnósticos u otra documentación de servicio relacionada con el participante, ya sea registrada en papel o en formato electrónico. Fuente: GDPR, OJ L 241, 17.9

Contraseña - una combinación de caracteres y números que permiten el acceso a un sistema informático o dispositivo móvil

Información personal[3] - es un tipo de Información Confidencial. Información Personal significa cualquier información relacionada con una persona física identificada o identificable (el 'interesado' o "Titular"). El término de Información Personal, para efectos de este Manual, es equivalente al de "Datos Personales", según lo define la Ley 1581 de 2012 y demás normativa aplicable en Colombia. Esto incluye todos los identificadores incluidos en la información de identificación personal (IIP).

Se puede identificar a una persona física en referencia a un identificador como un nombre, un número de identificación, datos de ubicación y un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona natural.

Los ejemplos de identificador incluyen:

- *Nombre (nombre y apellido, nombre del padre, apellido de soltera de la madre, alias, apodo, etc.),*
- *fecha de nacimiento lugar de nacimiento*
- *número de identificación personal (número de registro nacional, número de pasaporte, número de licencia de conducir, número de tarjeta de crédito),*
- *información de contacto: dirección (domicilio o lugar de trabajo), dirección de correo electrónico, números de teléfono,*
- *identidad digital (nombre de usuario de sitios web), dirección IP, etc.*
- *características personales (imagen fotográfica, huellas digitales, escritura a mano),*
- *identificación de propiedad personal (número de matrícula del vehículo)*

Procesamiento[4] - significa cualquier operación o conjunto de operaciones que se realiza sobre datos personales o sobre conjuntos de datos personales, ya sea o no por medios automatizados, como recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por

[3] HAI utilizará la definición de datos personales de la GDPR (Fuente: GDPR, OJ L 241, 17.9). Los 'datos personales' indicados en este manual son más amplios que, y por lo tanto, incluyen, la información de identificación personal (IIP).
[4] Fuente: GDPR, OJ L 241, 17.9

transmisión, difusión o puesta a disposición, alineación o combinación, restricción, borrado o destrucción. El término de Procesamiento, para efectos de este Manual, es equivalente al de "Tratamiento", según lo define la Ley 1581 de 2012 y demás normativa aplicable en Colombia.

Perfilado[5] - quiere decir cualquier forma de procesamiento automatizado de datos personales que consiste en el uso de datos personales para evaluar ciertos aspectos de la persona en relación con una persona física, en particular para analizar o predecir aspectos relacionados con el desempeño de esa persona física en el trabajo, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos.

Programa - se refiere a un individuo o entidad que realiza gestión de casos, diagnóstico, asesoramiento, tratamiento médico o derivación para tratamiento médico; capacitación del personal médico u otro personal en una instalación médica general cuya función principal es la gestión de casos, diagnóstico, tratamiento médico o derivación para el tratamiento médico y que son identificados como dichos proveedores.

Información privilegiada - es uno de los tres tipos de Información Confidencial. Incluye, pero no se limita a, información no pública que puede incluir planes de negocios, acuerdos, contratos, información financiera y de empleados, estrategias y técnicas. Los ejemplos de información no pública incluyen registros de personal, información bancaria y de registro y estrategias organizacionales o detalles operativos que pueden afectar negativamente la ventaja competitiva de la organización.

R

Reidentificación - El acto de asignar un código u otro medio de identificación de registro para permitir que la información desidentificada se vuelva a identificar, siempre que 1) el código u otro medio de identificación de registro no se derive de la información sobre el individuo ni esté relacionado con la misma, y no pueda de otra manera ser traducido para identificar al individuo; y 2) la entidad no utilice ni divulgue el código ni otros medios de identificación de registros para ningún otro fin, y que no divulgue el mecanismo para la reidentificación.

Investigación - Una investigación sistemática, que incluye desarrollo de investigación, pruebas y evaluación, diseñada para desarrollar o contribuir al conocimiento generalizable.

Restricción de procesamiento - significa el etiquetado de datos personales almacenados con el objetivo de limitar su procesamiento en el futuro. Fuente: GDPR, OJ L 241, 17.9.

S

Información Confidencial Personal (ICP) es un tipo de Información Confidencial. ICP se refiere a información que es privada y que podría dañar a un individuo si se hace pública. Es importante recordar que un dato no tiene que ser necesariamente cierto para causarle un gran daño a una persona; en ocasiones, la percepción de aquellos que buscan infligir daño es suficiente para representar una amenaza para la seguridad de un individuo. El término de Información Confidencial Personal, para efectos de este Manual, es equivalente al de "Datos Sensibles", según lo define la Ley 1581 de 2012 y demás normativa aplicable en Colombia.

El nivel de riesgo de las personas cuya ICP está comprometida varía mucho en función de su ubicación física y estado socioeconómico. Por lo tanto, la sensibilidad de los datos y las salvaguardas apropiadas deben considerarse caso por caso. A continuación, se proporcionan algunos ejemplos que generalmente se consideran ICP en diferentes culturas:

[5] Ibídem.

Tipos de ICP	*Información que podría ser la base de discriminación, acoso, controversia o persecución.*	*Información que puede llevar a una persona a hacer suposiciones sobre un aspecto sensible de la vida de otra persona*
Identidad, asociación, creencias.	*Origen o identidad racial o étnica, opiniones políticas, creencias religiosas o filosóficas, afiliación a partidos políticos o sindicatos, militancia*	La información sobre la ubicación o paradero de una persona (hogar, trabajo) o paradero, puede indicar el origen étnico y religioso de esa persona, lo que puede ser un punto de discordia y/o discriminación.
Datos de salud	*Datos genéticos, biométricos, datos de salud (pasados o presentes) que muestran una condición de salud física o mental* *a. registros médicos con diagnóstico, fórmula, detección/prueba)*	*Una hoja de papel que muestre que la provisión de atención médica puede llevar a alguien a creer que un individuo tiene cierta condición de salud física o mental.* *a. documentos que contienen afecciones médicas (notas del médico, etc.),* *b. recibos de pago, recordatorios de citas* *c. participación en programas de HAI (hoja de asistencia de grupo psicosocial, nota de asesoramiento sobre salud mental, etc.)*
Información de casos jurídicos	*La información que respalda un argumento jurídico es muy valiosa*	*Notas de consulta jurídica, registros legales, tarjetas de citas*
Vida sexual/orientación sexual	*La vida sexual u orientación sexual de una persona física.*	*Hojas de asistencia con los nombres de los participantes para actividades diseñadas para población VIH positiva (asociación de hombres homosexuales con el VIH)*

Subcontratista - Una persona a quien un afiliado delega una función, actividad o servicio, que no sea en calidad de miembro de la fuerza laboral de dicho afiliado.

T

Tercero - significa una persona física o jurídica, autoridad pública, agencia u organismo que no sea el interesado, el controlador, el procesador y las personas que, bajo la autoridad directa del controlador o procesador, están autorizados para procesar datos personales. Fuente: GDPR, OJ L 241, 17.9

Tratamiento Médico- La provisión, coordinación o administración de atención médica y servicios relacionados por parte de uno o más proveedores de atención médica, incluida la coordinación o administración de atención médica por un proveedor de atención médica con terceros; consulta entre proveedores de servicios de salud en relación con un paciente; o la derivación de un paciente para atención médica de un proveedor de servicios médicos a otro.

Transmisión de datos: la comunicación de los datos personales dentro o fuera del territorio nacional que tiene por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Transferencia de datos: cuando el responsable del tratamiento de datos personales envía información a los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país. La ley 1581 del 2012 prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos, excepto cuando el titular de los datos personales haya otorgado su autorización expresa e inequívoca para la transferencia, intercambio de datos de carácter médico cuando así lo exija el tratamiento

del titular por razones de salud o higiene pública, transferencias acordadas en el marco de tratados internacionales en los cuales Colombia sea parte (con fundamento en el principio de reciprocidad).

U

Uso - significa el intercambio, empleo, aplicación, utilización, examen o análisis de Información Confidencial al interior de una entidad que mantiene dicha información.

Usuario –Una persona o entidad con acceso autorizado.

W

Miembro de la fuerza laboral - significa miembro del personal a tiempo parcial o completo, consultor, asesor, evaluador, pasante, voluntario, trabajador estudiantil y otras personas cuya conducta (ya sea remunerada o no) en el desempeño del trabajo para Heartland Alliance International, está bajo la supervisión directa de la entidad.

Estación de trabajo - Un dispositivo informático electrónico como, por ejemplo, una computadora portátil o de escritorio o cualquier otro dispositivo que realice funciones similares y medios electrónicos almacenados en su entorno inmediato.

CAPÍTULO 1: PRINCIPIOS RECTORES

Este capítulo discute un conjunto de principios que justifican el desarrollo de políticas específicas de HAI y la necesidad de una mayor protección de la Información Confidencial. Menciona el principio de humanitarismo, el principio humanitario de "no hacer daño". Los donantes en el sector humanitario, como organizaciones internacionales, gobiernos, fundaciones e individuos, exigen cada vez más medidas de protección como condición para la financiación. Garantizar la privacidad y la seguridad de la información ha pasado de ser un gesto de buena voluntad a una cuestión de cumplimiento con los requisitos legales y de los donantes.

I. PRINCIPIO HUMANITARIO DE 'NO HACER DAÑO'

La filosofía de HAI y sus enfoques programáticos están firmemente arraigados en los principios de derechos humanos.

Uno de los principios más antiguos y fundamentales del humanitarismo es el principio de '*no hacer daño*'. El principio de '*no hacer daño'* reconoce los posibles efectos negativos de la acción humanitaria y obliga a quienes ofrecen servicios a tomar medidas preventivas para proteger a las personas que buscan ayuda. Ya sea intencional o no, el daño infligido a las personas necesitadas viola directamente el principio humanitario de '*no hacer daño'.*

En cualquier entorno, es extremadamente fácil difundir información entre las personas. La operación de programas de HAI a menudo involucra información, tanto en forma oral como escrita, que es altamente sensible. Mal manejada y revelada sin la debida autorización, la Información Confidencial puede causar serios daños a la reputación, financieros y físicos a aquellas personas cuya información ha sido mal manejada.

Los interesados pueden ser cualquier persona involucrada en el programa y la operación de HAI: miembros de la fuerza laboral de HAI (por ejemplo, personal a tiempo completo y parcial), afiliados (por ejemplo, socios y consultores) y, lo que es más importante, nuestros participantes. Dado que los participantes de HAI a menudo pertenecen a grupos de población vulnerables, el daño a su bienestar psicológico, reputación social y seguridad física resulta severo.

En todo caso, la violación de información privada y confidencial de un individuo es particularmente peligrosa, por las siguientes razones:

- a menudo conduce a consecuencias imprevistas que causan más daño a un individuo;
- a menudo aísla al individuo de su comunidad y apoyo social, lo que hace que sea más difícil recuperarse del daño, ya sea psicológico, reputacional o físico; y
- es casi imposible contener la difusión de información después de su violación en la era digital, lo que significa que el individuo puede sufrir daños una y otra vez durante mucho tiempo.

II. ENFOQUE CENTRADO EN EL PARTICIPANTE DE HAI

HAI atiende a una amplia variedad de participantes que son sobrevivientes de, y están en riesgo de sufrir abusos graves de los derechos humanos en muchos programas y oficinas de país, incluidos sobrevivientes de tortura, refugiados, minorías religiosas y étnicas, menores detenidos, niños soldados, mujeres y niñas vulnerables, víctimas de trata, personas LGBT, poblaciones clave en riesgo de contraer el VIH, y más. HAI adopta la cultura de que todas nuestras estrategias para el cambio se centran en los participantes en todas las etapas del trabajo: diseño, implementación, evaluación.

- HAI tiene el deber de prevenir y mitigar cualquier impacto negativo de su acción en la población afectada, de acuerdo con el principio humanitario de *'no hacer daño'*[6].

- HAI está comprometido con un enfoque basado en los derechos: 1) promoción de todos los derechos y la dignidad de la población afectada; y 2) empoderamiento de la población afectada.

Este enfoque se deriva de la filosofía de los principios de derechos humanos de HAI, que guía sus políticas y prácticas organizacionales para priorizar siempre el bienestar de los participantes por encima de todo. En consecuencia, HAI defiende uno de los principios más antiguos y fundamentales del humanitarismo, el principio de 'no hacer daño'. El principio de 'no hacer daño' exige a todos los actores humanitarios reconocer los efectos negativos de la acción humanitaria y tomar medidas preventivas para proteger a las personas que buscan ayuda.

Como parte de este esfuerzo:

> *HAI reconoce la privacidad y seguridad de la información relacionada con los participantes como un elemento crucial de la seguridad y sentido de seguridad y dignidad de los participantes.*
>
> *HAI tiene el deber de prevenir y mitigar cualquier impacto negativo de su acción en la población afectada que surja de la recopilación, el registro y el intercambio de información personal.*

La mejor solución, y algunos pueden argumentar que es la única, para la violación de Información Confidencial es la prevención. La ocurrencia frecuente de violaciones puede socavar la confianza entre HAI y sus participantes, donantes, organizaciones asociadas y partes interesadas locales. En consecuencia, es responsabilidad de HAI —todos los miembros de la fuerza laboral y afiliados— practicar la debida diligencia para proteger cualquier información de naturaleza sensible que puedan encontrar durante la operación de HAI de la violación, ya sea que ocurra a través de una divulgación accidental o un ataque de ciberseguridad planificado.

III. CUMPLIMIENTO

Además del argumento ético, existen factores relacionados con las operaciones que obligan a HAI a establecer e implementar políticas más estrictas sobre seguridad de la información, como:

- ***Requerimientos legales:*** la violación de leyes locales de privacidad de los países en que opera HAI puede representar una amenaza directa a la legalidad de la operación de HAI. Además, violar la ley perjudica la relación que HAI ha establecido con las partes interesadas locales, como las organizaciones locales de la sociedad civil (OSC), las agencias gubernamentales y las fuerzas del orden.

- El GDPR (Reglamento general de protección de datos 2016/679) es una norma de la legislación de la UE sobre protección de los datos y la privacidad de las personas. La jurisdicción extendida del GDPR aplica a todas las empresas que realizan:

    1) procesamiento de los datos personales de los interesados que residen en la Unión, independientemente de la ubicación de la empresa.
    2) procesamiento de datos personales por parte de controladores y procesadores en la UE, independientemente de si el procesamiento se lleva a cabo en la UE o no.

[6] El principio humanitario de 'no hacer daño' se puede encontrar bajo numerosos principios fundamentales en el sector internacional humanitario/de derechos humanos, tales como: Código de conducta para el movimiento internacional de la Cruz Roja y de la Media Luna Roja y las organizaciones no gubernamentales (ONG) en materia de socorro en casos de desastre; Principios de la Federación Internacional; OCHA sobre principios humanitarios; el Proyecto SPHERE; la Asociación de Responsabilidad Humanitaria; la Norma Humanitaria Esencial; la Resolución de la Asamblea General 46/182

3) procesamiento de datos personales de los interesados en la UE por un controlador o procesador no establecido en la UE, donde las actividades se relacionan con: ofrecer bienes o servicios a ciudadanos de la UE (independientemente de si se requiere pago) y con el monitoreo del comportamiento que tiene lugar dentro de la UE.
4) Las empresas no pertenecientes a la UE que procesan los datos de ciudadanos de la UE también deben designar un representante en la UE.

- *Cumplimiento de donantes:* Los principales donantes del sector humanitario, tales como organizaciones internacionales, gobiernos, fundaciones e individuos, exigen cada vez más medidas de protección como condición para la financiación. Los donantes actuales y futuros de HAI requieren que los beneficiarios de sus subvenciones se adhieran a cierto nivel de medidas de protección de datos basadas en el estándar Esfera. Garantizar la privacidad y la seguridad de la información ha pasado de ser un gesto de buena voluntad a una cuestión de cumplimiento con los requisitos legales y de los donantes.

IV. MEJORES PRÁCTICAS EN EL SECTOR HUMANITARIO

Las principales agencias del sector humanitario expresan su preocupación por las amenazas contra la privacidad y la seguridad de la información hoy más que nunca. Esto ocurre en un momento en que el mundo está siendo testigo de un creciente número de ataques cibernéticos por parte de piratas informáticos y regímenes opresivos, y el reciente alboroto respecto al uso de tácticas invasivas por parte de empresas de redes sociales para recopilar, almacenar y vender datos personales a entidades con agenda comercial y política. Las principales agencias humanitarias han comenzado a publicar directrices y protocolos sobre las mejores prácticas para proteger la información personal durante la operación humanitaria. Esta tendencia en el sector humanitario hacia medidas más estrictas de privacidad y seguridad de la información es parte del movimiento global hacia leyes y regulaciones locales de privacidad fortalecidas.

CAPITULO 2: INFORMACIÓN CONFIDENCIAL

El capítulo anterior revisó los principios rectores que respaldan la justificación de la política de HAI sobre privacidad y seguridad de la información para la necesidad de desarrollar un conjunto de normas que se alineen con el contexto y las prácticas cotidianas en la operación y programación de HAI.

Los miembros de la fuerza laboral y afiliados de HAI acceden, editan y revisan de manera rutinaria documentos que contienen Información Confidencial. Esto puede ser cualquier cosa desde documentos internos de HAI, datos personales[7] reunidos para archivos de casos, notas que contienen información confidencial personal (ICP)[8]o información privilegiada. Dependiendo de la función laboral de cada quien, también se pueden crear archivos físicos o digitales y otros contenidos multimedia que contengan dicha información (por ejemplo, tomar notas durante las reuniones, grabar voz, tomar fotos o videos, hacer fotocopias).

Este capítulo proporciona la definición de información 'sensible' en el contexto de HAI, la política de no divulgación, sus excepciones y el deber de discreción y conducta del personal.

I. ¿QUÉ ES LA "INFORMACIÓN CONFIDENCIAL"?

Los proyectos de HAI a menudo implican acceder y revisar archivos electrónicos o físicos que pueden contener datos personales, información confidencial personal (ICP) o información privilegiada. La fuerza laboral y los afiliados de HAI a menudo también crean documentos y medios que contienen dicha información (incluyendo tomar notas, grabar voz, tomar fotos o videos, hacer fotocopias).

Información Confidencial quiere decir colectivamente datos personales, información confidencial personal (ICP) e información privilegiada.

Debido a la naturaleza del programa de HAI, la información altamente sensible que pertenece a un participante o a HAI, denominada colectivamente “Información Confidencial” en este documento, a menudo se recopila, registra y comparte en forma oral y escrita.

Como organización, HAI utiliza el correo electrónico como su principal canal de comunicación. La comunicación por correo electrónico ya es en sí misma muy vulnerable a los ataques cibernéticos (piratería, phishing, etc.), y cualquier usuario de correo electrónico puede exponer fácilmente cierta información a personas no autorizadas. Sin medidas de discreción y protección, es muy probable que se produzca una violación de la información, y el costo de mitigación puede ser astronómico.

Cuando ocurre una violación, puede causar serios daños financieros y reputacionales a la organización y a las personas que trabajan para/con la organización. En todo caso, la violación de información privada y confidencial de un individuo es particularmente peligrosa, por las siguientes razones:

- a menudo conduce a consecuencias imprevistas que causan más daño a un individuo;
- a menudo aísla al individuo de su comunidad y apoyo social, lo que hace que sea más difícil recuperarse del daño, ya sea psicológico, reputacional o físico; y

[7] Los datos personales se refieren a la información que se puede utilizar para distinguir o rastrear la identidad de un individuo, ya sea independientemente o cuando se combina con otra información personal o de identificación. Para obtener una definición detallada, consulte el Glosario de Términos en el manual de HAI.
[8] La información confidencial personal (ICP) se refiere a la información que es privada o que podría dañar a un individuo si se hace pública. Los ejemplos incluyen: origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, y el procesamiento de datos genéticos, datos biométricos, datos sobre la salud (por ejemplo, salud mental o estado de VIH), datos sobre la vida u orientación sexual de una persona natural.

- es casi imposible contener la difusión de información después de su violación en la era digital, lo que significa que el individuo puede sufrir daños una y otra vez durante mucho tiempo.

En el contexto del programa de HAI, esto puede causar daños críticos al bienestar de los participantes, que a menudo ya pertenecen a un grupo de población vulnerable. El daño a su bienestar psicológico, reputación social y seguridad física puede ser grave e irreparable.

II. POLÍTICA DE NO DIVULGACIÓN DE INFORMACIÓN CONFIDENCIAL

El programa de HAI abarca países con diferentes perspectivas legales y culturales sobre la privacidad y la seguridad de la Información Confidencial. Para establecer un entendimiento común entre sus oficinas en los países, HAI basará su política en los principios mencionados en el capítulo anterior: el principio de *'no hacer daño'*, el estándar mínimo necesario, y la filosofía de HAI de priorizar los derechos de los participantes.

La no divulgación de Información Confidencial significa que la Información Confidencial no debe compartirse con otras personas que no tienen una razón legítima para conocer dicha información.

Todos los miembros de la fuerza laboral y afiliados de HAI deben seguir la regla de no divulgación de Información Confidencial:

- *La obtención, divulgación y/o uso de cualquier Información Confidencial para uso personal está estrictamente prohibida bajo cualquier circunstancia.*
  El uso de Información Confidencial para beneficio personal o el beneficio de otra persona no es ético, va contra las políticas de HAI, y en muchos países puede ser ilegal. Los miembros de la fuerza laboral que usan, acceden a o divulgan Información Confidencial de manera inadecuada pueden estar sujetos a medidas disciplinarias, que pueden incluir la terminación del empleo o afiliación, incluso si no se obtuvo ningún beneficio real de dicho uso o divulgación.

- *El uso de cualquier Información Confidencial debe estar restringido a la operación y el servicio de HAI.*
  En todo momento, los miembros de la fuerza laboral y los afiliados que entran en contacto con Información Confidencial, ya sea obtenida o intercambiada verbalmente, electrónicamente o en formato escrito, deben tomar las medidas apropiadas y ejercer la debida diligencia para proteger la Información Confidencial.

- *Solo el personal autorizado debe tener acceso a la Información Confidencial.*

  Los miembros de la fuerza laboral y los afiliados cuya función laboral central es acceder a la Información Confidencial (por ejemplo, trabajadores sociales, psicólogos, administradores de casos, trabajadores de salud comunitarios, etc.) no están obligados a obtener autorización cada vez que accedan a Información Confidencial. El acceso está limitado a solo un conjunto de información directamente relacionada con la descripción del trabajo de cada quien.

  Todos los demás miembros de la fuerza laboral y afiliados de HAI deben primero solicitar y obtener una autorización por escrito del personal apropiado (por ejemplo, supervisor, líder del país, gerente de seguridad, etc.) y firmar el formulario del acuerdo de confidencialidad y seguridad.

  'Acceso' en este caso incluye:

  a) *escuchar, leer o entrar en contacto con Información Confidencial;*
  b) *recopilar Información Confidencial en forma verbal o escrita (tanto digital como física);*
  c) *crear o copiar contenido que contenga Información Confidencial. 'Contenido' puede incluir, pero no está* limitado a:

- *archivos electrónicos*: documentos de Word, hojas de cálculo de Excel, diapositivas de PowerPoint, archivos de mensajes de correo electrónico, etc.
- *documentos físicos*: notas escritas a mano, documentos impresos, copias en papel del documento original, post-its, etc.
- *medios: archivos de audio, fotografías (tanto electrónicas como impresas), archivos de video, etc.*

d) almacenar de contenido que contenga Información Confidencial en forma física (por ejemplo, un lugar de almacenamiento, cajón, la cajuela de un vehículo, etc.) y/o configuración en línea (por ejemplo, base de datos, unidad compartida, dispositivo móvil, etc.);

e) compartir o divulgar contenido que contenga Información Confidencial a cualquier persona o entidad.

III. EXCEPCIONES A LA POLÍTICA DE NO DIVULGACIÓN

La política de no divulgación de Información Confidencial no se aplica a ninguna Información Confidencial que:

- es o se vuelve de conocimiento público general, sin acción por parte de los miembros de la fuerza laboral;
- generalmente es divulgada a terceros por Heartland Alliance International;
- se aprueba para su liberación por autorización escrita del Director Ejecutivo o la Junta;
- es revelada por un portavoz autorizado de Heartland Alliance International según lo permitido;
- es conforme a una citación, orden de la autoridad judicial o administrativa local; o
- está relacionada con procedimientos judiciales en los que Heartland Alliance International, sus afiliados o miembros de la fuerza laboral son parte.

Aviso importante: Esta política no tiene la intención de restringir o prohibir, de ninguna manera, la capacidad y obligación de los miembros de la fuerza laboral ni interfiere con los derechos otorgados a un individuo para revelar información que:

- se requiere que se divulgue para la seguridad física inmediata de los participantes;
- debe ser revelada de acuerdo con las leyes de reporte obligatorio en el país de operación;
- debe ser divulgada para informar sospechas de fraude, desperdicio o abuso; o
- se hace de manera confidencial a funcionarios gubernamentales o abogados con el único fin de informar o investigar una presunta violación de la ley.

IV. DEBER DE DISCRECIÓN & CONDUCTA DEL PERSONAL

Alcance: Esta política aplica a todos los miembros de la fuerza laboral de Heartland Alliance International y sus afiliados.

Heartland Alliance International (HAI) se compromete a proteger la privacidad y la seguridad de la información de nuestro personal y participantes al garantizar que los miembros de su fuerza laboral y afiliados, incluidos consultores, personal de organizaciones asociadas, voluntarios o pasantes, reciban capacitación adecuada y periódica sobre la importancia de la privacidad y seguridad.

Cualquier miembro de la fuerza laboral o afiliado de HAI puede escuchar, leer, crear o entrar en contacto con una información en formato electrónico, físico o verbal que contenga Información Confidencial. Todos los miembros de la fuerza laboral y afiliados de HAI, incluidos los consultores, el personal de organizaciones asociadas, los voluntarios o los pasantes, tienen el deber de discreción y conducta del personal. Los infractores de cualquier política y protocolo en el anexo de HAI o cláusulas referenciadas en el manual de HA están sujetos a medidas disciplinarias, que pueden incluir la desvinculación.

- Los miembros de la fuerza laboral y los afiliados deben reducir al mínimo el uso, las solicitudes, el almacenamiento y las divulgaciones de Información Confidencial, interactuando con Información Confidencial **solo cuando es necesario** para el correcto desempeño de las funciones de la organización. La Información Confidencial no debe recopilarse, almacenarse ni compartirse para fines de conveniencia.

- Los miembros de la fuerza laboral y afiliados deben mantener cualquier Información Confidencial en fideicomiso y no usarla ni divulgarla, directa o indirectamente, excepto cuando sea necesario en el desempeño de las funciones de Heartland Alliance International, o según lo exija la ley o el contrato.

- Los miembros de la fuerza laboral y afiliados tienen estrictamente prohibido el uso de cualquier información del participante para uso personal, cualquier otro fin que no sea la operación y el servicio de HAI.

- Los miembros de la fuerza laboral y afiliados que hagan uso, accedan o divulguen Información Confidencial de forma inadecuada pueden estar sujetos a medidas disciplinarias, que pueden incluir la terminación del empleo o la afiliación, incluso si no se obtuvo ningún beneficio real de dicho uso o divulgación.

- Los miembros de la fuerza laboral y afiliados no pueden eliminar Información Confidencial de una oficina/ ubicación de HAI, ni duplicar Información Confidencial, a menos que estén expresamente autorizados para hacerlo o según sea necesario en el desempeño de las funciones laborales de la persona. Una vez que los materiales que contienen Información Confidencial están autorizados para su eliminación, el miembro de la fuerza laboral debe proteger los materiales/propiedad y controlar el acceso según sea necesario.

- Los miembros de la fuerza laboral y afiliados no buscarán obtener ninguna Información Confidencial relacionada con ningún asunto que no implique o esté relacionado con las funciones laborales de la persona.

- La Información Confidencial no puede ser manipulada, alterada o destruida maliciosamente, excepto cuando esté autorizada y documentada según la política de retención de datos de HAI.

- Al finalizar cualquier asignación o contrato, o según lo indique un supervisor, los miembros de la fuerza laboral y afiliados devolverán todos los materiales y copias a su ubicación adecuada.

- Las solicitudes de entidades o personas externas para la divulgación de Información Confidencial deben dirigirse de inmediato al personal apropiado, a menos que el miembro de la fuerza laboral y afiliados tengan la autoridad para responder a tales solicitudes.

- Todos los afiliados de HAI, tales como organizaciones asociadas, consultores, pasantes y voluntarios, deberán leer y firmar el formulario o las cláusulas de reconocimiento de confidencialidad y seguridad como parte de su contrato de empleo/ consultoría/subcontratación.

- Se espera que todos los miembros de la fuerza laboral cumplan con los términos de la política al leer y firmar el **Acuerdo de reconocimiento de confidencialidad y seguridad.**

CAPÍTULO 3: PROTOCOLO DE PROCESAMIENTO DE LA INFORMACIÓN [9]

Alcance: Esta política se aplica a todos los miembros de la fuerza laboral de Heartland Alliance International y sus afiliados.

Diariamente, los miembros de la fuerza laboral y afiliados de HAI interactúan con Información Confidencial en varias capacidades. Este documento llamará a esta interacción *'procesamiento'.*

Procesamiento se refiere a cualquier operación realizada sobre un dato, como recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación (es decir, transmisión de datos por correo, correo electrónico, etc.), difusión o borrado.

La mayoría de las veces, la violación accidental de la información ocurre principalmente debido a la falta de conciencia de las personas sobre el comportamiento de riesgo o la falta de precaución. En el contexto de la programación de HAI, la violación de Información Confidencial, en particular los datos personales y la información confidencial personal (ICP), es un riesgo demasiado grande para correr; por lo tanto, es responsabilidad de todos los miembros de la fuerza laboral y afiliados de HAI aprender e implementar protocolos diseñados para proteger los aspectos más sensibles de la vida de los participantes.

Una regla de oro es el principio del **mínimo necesario**, el estándar universal para la protección de datos. Esto significa que los miembros de la fuerza laboral y los afiliados deberían reducir al mínimo el uso, las solicitudes, el almacenamiento y las divulgaciones de Información Confidencial, y deberían limitar su interacción con Información Confidencial al mínimo necesario para el desempeño adecuado de las funciones de la organización. La Información Confidencial no debe recopilarse, almacenarse ni compartirse para fines de conveniencia.

Este capítulo proporciona un conjunto de protocolos a seguir al procesar Información Confidencial: reunión/recolección, control de almacenamiento/acceso y transmisión—utilizando los siguientes términos:

Agente es un individuo o un grupo de individuos que buscan obtener o acceder a cierta información.

Contenido es una información documentada en varias formas de medios, tales como: voz hablada, escritos, fotografías, videos, grabaciones de audio, etc. El contenido es el producto de la actividad de recopilación de información.

Fuente de datos es una persona o un objeto que proporciona información a un agente.

[9] Este capítulo utilizará los términos 'información' y 'datos' indistintamente.

I. PROTOCOLO DE RECOPILACIÓN/RECOLECCIÓN DE INFORMACIÓN

La recopilación de información quiere decir cualquier acción tomada con el propósito de capturar cierta información.

En el contexto de la operación de HAI y las actividades del programa, la recopilación de información puede ser cualquier cosa, desde la recopilación de datos para evaluación de necesidades, la realización de encuestas a participantes, la toma de notas escritas a mano, la grabación de una conversación, el llenado del formulario de admisión o la toma de una fotografía /video.

1. Prueba del mínimo necesario

- La actividad de recopilación de información primero debe pasar la prueba estándar del *mínimo necesario.* El agente debe preguntar si la recopilación de información es necesaria para la operación de HAI y su misión de promover el bienestar de los participantes.

- La recopilación de información y la creación de contenidos deben realizarse de manera que minimice el riesgo, si lo hay, para la fuente de datos y/o el interesado. Cualquier actividad de recopilación de información que ocurra en una configuración de seguridad de riesgo medio o alto primero debe obtener la autorización del Jefe de Seguridad de HAI.

- El número de personas que recopilan información (por ejemplo, agrimensores, trabajadores sociales que completan la admisión, etc.) debe ser mínimo.

- La cantidad de información recopilada debe ser mínima. Solo debe reunir la información necesaria para el objetivo de la actividad. No recopile información periférica innecesaria haciendo preguntas no relacionadas, tomando notas sobre detalles no relacionados, tomando fotos de la casa del participante, etc.

2. Recopilación de datos del participante: Proceso de consentimiento

En la programación de HAI, recopilar *información personal*[10] o *información personal confidencial*[11] de manera segura y confidencial no es una tarea simple: los recolectores de datos deben preguntar a las personas vulnerables, a menudo traumatizadas, sobre un tema altamente sensible y considerar el riesgo para el sujeto y/o la fuente de datos al mismo tiempo.

Para evitar poner en riesgo la fuente de los datos, el agente, los miembros de la fuerza laboral y afiliados de HAI y la organización, es mejor incorporar las mejores prácticas antes de que comience la actividad de recopilación de información. Es responsabilidad del agente completar los siguientes procedimientos *antes de* iniciar cualquier actividad de recopilación de información:

Paso 1: El agente proporciona una justificación de por qué dicha actividad de recopilación de información es necesaria para la operación/programa de HAI. El agente debe presentar una declaración por escrito:

a. para qué se utilizará la información (por ejemplo, objetivo de la actividad);

[10] Datos personales significa cualquier información relacionada con una persona física identificada o identificable (un 'interesado'); una persona física identificable es aquella que puede ser identificada, directa o indirectamente. Para más información ver Glosario de Términos.

[11] La información confidencial personal quiere decir cualquier información que sea privada y que podría dañar a un individuo si se hace pública. Para ejemplos, ver Glosario de Términos.

b. cómo se recopilará la información (por ejemplo, fuente de datos, frecuencia de recopilación, recolectores de datos)
c. cómo la información, una vez recopilada para el propósito de HAI, se enviará a HAI
d. si los beneficios superan los riesgos (tanto a nivel individual como organizacional); y
e. una garantía por escrito de los recopiladores de datos para cumplir con la política de HAI durante la recopilación de datos, y de no recopilar, acceder a o compartir la Información Confidencial para ningún fin más allá de lo autorizado.

Paso 2: El agente presenta la declaración a 1) su supervisor, 2) un miembro del personal directivo superior del país donde se realizará la recopilación de información, y 3) el gerente del proyecto correspondiente.

a. Debe discutir la declaración escrita que justifica la recolección.
b. Discutir los beneficios y riesgos para las personas involucradas y para HAI. Los puntos focales directos deben brindar insumos sobre esta discusión (por ejemplo, trabajadores sociales, personal que interactúa directamente con los participantes).

Paso 3: Una vez que todos estén de acuerdo en que los beneficios superan los riesgos, se puede contactar a la fuente de datos.

Obtención del consentimiento de los participantes de HAI: el trabajador social designado y el gerente del proyecto (si corresponde) deben primero aprobar la actividad de recopilación de información. El proceso de consentimiento puede ser facilitado por el agente o el trabajador social, pero independientemente del facilitador, el trabajador social debe estar presente durante el proceso de consentimiento. Si el trabajador social no puede estar presente debido a circunstancias especiales, el agente debe notificar al trabajador social lo antes posible. Para los participantes que pueden tener desafíos adicionales para comprender el consentimiento debido a su edad, estado de discapacidad y otros factores de vulnerabilidad, también debe estar presente un cuidador que pueda abogar por el participante.

Paso 4: Una vez en contacto con la fuente de datos, el agente debe explicar primero el objetivo de la actividad de recopilación de información y la naturaleza de la misma. Indicar claramente qué información están buscando los agentes. Si la fuente de datos expresa interés en proporcionar la información, puede darse inicio al proceso de consentimiento informado.

Nota 1: asegúrese de que la fuente de datos sea capaz de dar su consentimiento. Muchos factores pueden invalidar el consentimiento (por ejemplo, la edad, condición de discapacidad, dinámica de poder, etc.) dependiendo de los requisitos legales locales. Asegúrese de que la fuente de datos pueda comunicarse libremente con los agentes; de lo contrario, se debe proporcionar un traductor para explicar las condiciones de consentimiento en la lengua materna de la fuente de datos.

Nota 2: Dependiendo del medio a través del cual se recopile o recolecte la Información Confidencial, variará el mecanismo a través del cual se recaude la Autorización del Titular. Si el medio es presencial, el Titular deberá firmar, de su puño y letra, el formulario de consentimiento estándar de HAI (Paso 5 siguiente). Si la recolección es por medio de llamada telefónica, grabación de video o correo electrónico, se deben seguir los pasos previstos en el numeral 3 siguiente de este punto I.

Paso 5: Revisar el formulario de consentimiento estándar de HAI completo. Antes de solicitar el consentimiento después de explicar el contenido, el facilitador debe preguntar si la fuente de datos potencial tiene alguna pregunta. Una vez que la fuente de datos expresa que comprende completamente la condición

del consentimiento, los facilitadores pueden solicitar formalmente su consentimiento y firma/huella digital en el formulario de consentimiento de HAI.

Nota: La coerción, explícita o implícita, o las falsas promesas hechas en cualquier etapa del proceso de consentimiento invalidan el consentimiento otorgado por el participante.

Paso 6: Los agentes deben proporcionar una copia del formulario de consentimiento firmado a 1) la fuente de datos; y 2) al trabajador social. Los agentes también deben proporcionar su información de contacto para cualquier pregunta que pueda surgir en el futuro.

Nota: En Colombia, el formulario de autorización debe prever expresamente el destino que se le dará a la Información Confidencial y el uso para el cuál se está recopilando o recolectando. Dentro de los usos o destinos permitidos de la Información Confidencial que se le deben indicar al Titular, están:

- Contactar a los participantes o Titulares para ofrecer los servicios, confirmar citas, proveer servicios (proveemos servicios telefónicos), solicitar información relacionado con su caso, etc.;
- Contactar a los participantes o Titulares para realizar encuestas (encuestas de satisfacción, etc.);
- Contactar a los participantes o Titulares para resolver reclamos, quejas, etc.;
- Remitir a los participantes o Titulares a otros proveedores de servicios para los servicios que necesitan, pero HAI no ofrece;
- Procesar datos para presentar números agregados a nuestros donantes y para informes externos (nunca publicamos datos individuales, solo información agregada, como "Brindamos servicios de asesoramiento para 10,000 personas" etc.);
- Analizar datos para mejorar la calidad del servicio;
- Es posible que, en el caso de una auditoría del donante, nuestros donantes deban revisar nuestros registros, incluidos los datos de los participantes a nivel individual. Es poco probable, pero nuestros contratos requieren que pongamos a disposición de nuestros donantes cualquier información si la solicitan;
- Cumplimiento de la ley colombiana o extranjera y de las órdenes de autoridades judiciales y administrativas;
- Compartir Datos Personales con, o transferir o transmitir a, terceros para que éstos puedan darle Tratamiento, con quienes tenemos relaciones comerciales y/o contractuales, a título gratuito y/u oneroso, en Colombia o en el exterior.

3. Consentimiento para fotografías/video/grabaciones de audio

Debido a la naturaleza delicada de los programas de HAI, cada agente debe seguir las pautas y los procedimientos descritos en esta política antes de crear los contenidos en medios al tratar de recopilar información mediante fotografías, grabaciones de video o audio, o de otra manera obtener imágenes de los participantes, visitantes o miembros de la fuerza laboral. Cualquier actividad de recopilación de información que implique la creación de contenidos multimedia como fotografías, grabaciones de video/audio y otras imágenes de participantes, visitantes y

miembros de la fuerza laboral, seguirá la Política de HA que proporciona un protocolo detallado basado en una variedad de escenarios y propósitos.

La forma de obtención de la Autorización del Titular para el Tratamiento de Datos en Colombia, varía dependiendo del medio por el que se obtenga dicha Autorización.

Si se trata de llamada telefónica o grabaciones de audio:

1. Debe ser grabada. Para el efecto, al comienzo de la llamada se debe advertir al Titular o participante que la llamada está siendo grabada. Se debe pedir la autorización para continuar adelante, manifestando y preguntando: "Esta llamada está siendo grabada para efectos de su monitoreo y verificación. ¿Está Usted de acuerdo en continuar en estas condiciones?
2. Con posterioridad, se debe solicitar la autorización para el Tratamiento de Datos Personales, para lo cual se debe manifestar y preguntar: "Los Datos Personales que sobre Usted se recolecten, recopilen y almacenen en esta llamada y por cualquier medio, serán tratados de acuerdo con la Política de Tratamiento de Datos de HAI y de acuerdo con la ley aplicable en Colombia. ¿Está Usted de acuerdo en autorizar el Tratamiento de sus Datos personales en esta forma?"
3. Las respuestas del Titular deben ser expresas, manifestando un sí o un no, independientemente de que se hagan adiciones o aclaraciones a la respuesta.

Si se trata de una grabación de video en cualquiera de las instalaciones de HAI en Colombia, debe existir un aviso con el siguiente texto en un lugar visible:

"AVISO DE PRIVACIDAD

Usted está siendo videograbado por Heartland Alliance International ("HAI") para efectos de procurar la seguridad de los bienes y personas que ingresan, permanecen y salen de este establecimiento y con la finalidad de poder identificar, investigar y combatir la eventual comisión de delitos.

Las imágenes captadas serán tratadas de acuerdo con la ley y con la política de tratamiento de datos personales de HAI, que Usted puede consultar para mayor detalle en heartlandalliance.org/hai-manual-privacidad-seguridad-colombia-2020

Al ingresar al establecimiento, luego de haber leído este aviso, entendemos por su conducta inequívoca, que Usted nos confiere su autorización para que le demos tratamiento a sus datos personales. En su calidad de titular, Usted podrá ejercer los derechos que le confiere la ley, de acuerdo con lo previsto en la misma y en la referida Política.

Las imágenes serán conservadas por HAI durante el tiempo que sea necesario para cumplir con la finalidad anteriormente descrita. Las imágenes serán sometidas a estrictas medidas de seguridad, en los términos de la Política de HAI."

Si se trata de un correo electrónico:

1. En el primer contacto que se tenga con el Titular por este medio, se le debe advertir que se recopilarán Datos Personales y que los mismos serán tratados de acuerdo con la política de datos de la entidad.
2. Para el efecto, se le debe enviar un primer correo con un texto de este estilo:

"En HAI nos preocupamos por la seguridad de sus datos personales. Es por eso que, antes de continuar con nuestra interacción, queremos contar con su autorización para dar tratamiento a sus datos personales de conformidad con la política de tratamiento de datos de HAI.

Si está de acuerdo con ello, le solicitamos contestar a este correo electrónico en forma expresa manifestando que acepta dicho Tratamiento. En todo caso, le informamos que, si Usted contesta a este correo con cualquier contenido, o de cualquier forma se pone en contacto con HAI o utilice o navegue a través de su página web o cualquier otra de sus plataformas digitales, entenderemos que Usted está confirmando su autorización para que podamos dar tratamiento a sus datos de conformidad con la Política de Tratamiento de Datos de HAI y está aceptando la referida política."

3. El correo electrónico debe ser conservado y almacenado como la prueba de la existencia de la autorización, en los términos del "Protocolo de Almacenamiento" previsto en el acápite siguiente.

II. PROTOCOLO DE ALMACENAMIENTO/ACCESO A LA INFORMACIÓN

Parte de la Información Confidencial puede requerir el acceso regular de miembros de la fuerza laboral y afiliados para llevar a cabo la función de cada quien. En tal caso, los archivos digitales/físicos que contienen Información Confidencial deben estar protegidos en todo momento.

1. Prueba del mínimo necesario

El almacenamiento físico (por ejemplo, gabinetes, almacenamiento) o electrónico (por ejemplo, computadoras, unidades de disco, etc.) nunca son lugares seguros para la Información Confidencial. Estos documentos corren un riesgo constante de pérdida, robo o daño. Se recomienda guardar solo los documentos necesarios y eliminar los archivos innecesarios para evitar la violación de la información. Para reducir el riesgo de incumplimiento de la Información Confidencial, se debe:

- Minimizar la cantidad de Información Confidencial guardada en almacenamiento físico (por ejemplo, gabinetes, contenedores de almacenamiento) o electrónico (por ejemplo, computadoras, unidades de disco, etc.)

- Revisar regularmente el sitio de almacenamiento para purgar archivos/documentos innecesarios. Cualquier archivo guardado en almacenamiento físico y electrónico que no se use de inmediato para propósitos de HAI o sus copias originales (puede ser necesario considerarlo y consultarlo con otro miembro del personal de HAI) debe ser eliminado y destruido.

- Al guardar nuevos documentos/archivos con Información Confidencial, cree un informe de divulgación[12] por archivo Esto permitirá a los gestores de datos realizar un seguimiento de cuándo y quién accedió a la Información Confidencial.

- Minimizar la cantidad de personas que acceden a la Información Confidencial. Las personas que no tienen la autorización adecuada no deben tener acceso a la Información Confidencial.

2. Protocolo de acceso

Dependiendo de la función de cada quien, los miembros de la fuerza laboral y afiliados de HAI pueden tener que acceder regularmente a la Información Confidencial para cumplir con sus tareas diarias. En tal caso, estas personas serán consideradas como "actores preaprobados". Por ejemplo, un gestor de casos necesitará revisar con frecuencia los archivos de casos que contienen información privada y confidencial de los participantes. Un empleado de recursos humanos puede necesitar acceder a los archivos de personal que pertenecen a los miembros de la fuerza laboral de HAI. Los altos directivos y los empleados del departamento de finanzas pueden necesitar acceso a documentos financieros y legales sensibles de HAI. En caso de duda, las personas no deben compartir la información con los agentes que solicitan acceso. Si surge alguna confusión, consulte con el punto focal senior de M&E en cada oficina de país o en la sede principal.

- Para que cualquier miembro de la fuerza laboral y afiliado de HAI tenga acceso a Información Confidencial, los agentes[13] deben cumplir con uno de los siguientes requisitos antes de acceder a la información:

[12] Un documento que se mantiene para cada participante que registra qué Información Confidencial fue utilizada/compartida/revelada a quién por HAI.

[13] Un agente es un individuo/grupo que busca recopilar cierta información. En este caso, los agentes serían miembros de la fuerza laboral o afiliados de HAI;

a) el nombre, cargo y nivel de acceso[14] del agente está incluido en la lista de "actores preaprobados"; o
b) el agente ha obtenido una prueba de autorización del supervisor del agente y del personal superior de HAI

- Los miembros de la fuerza laboral y afiliados de HAI necesitan una mención explícita en la descripción de su trabajo y la aprobación de sus supervisores para registrarse como actores preaprobados.

- Al comienzo de un proyecto, el equipo de programa (en el país y la sede) debe trabajar con los puntos focales de monitoreo y evaluación (M&E) para elaborar un plan de control de acceso. Esto dependerá de los roles de los miembros de la fuerza laboral y afiliados de HAI, así como de las mejores prácticas de M&E. En este proceso, la naturaleza de la Información Confidencial debe clasificarse y la lista de personas que requieren acceso regular debe documentarse para cada categoría. Esta lista de actores preaprobados debe ser aprobada tanto por los altos funcionarios de puntos focales de M&E en el país y en la sede.

3. Protocolo de almacenamiento

INFORMACIÓN/DATOS DEL PARTICIPANTE

- Cualquier contenido relacionado con individuos: *información personal*[15] o *información personal confidencial*[16] la mayoría de archivos de casos (es decir, formularios de admisión, notas de tratamiento médico, hojas de asistencia con nombres de participantes, formularios de informe de incidentes, etc.) deben almacenarse solo después de que los agentes obtengan el consentimiento de la fuente de datos: el participante. Se debe buscar el consentimiento dentro del contexto de una prestación de servicios y derivación.

- La información de los participantes debe estar protegida en todo momento y solo se debe acceder a la misma con autorización previa (más información en la sección "protocolo de intercambio de información" a continuación). Información accesible para miembros de la fuerza laboral y afiliados de HAI cuya función principal de trabajo es acceder a dicha información.

  Por ejemplo, los abogados que prestan servicios legales a un participante no deben tener acceso a la información en los archivos de caso de los participantes que no se refiera a cuestiones jurídicas, tales como notas de sesiones de terapia de salud mental. Solo el psicólogo que tomó las notas y el trabajador social designado deben tener acceso a las notas.

PAPEL/MEDIOS IMPRESOS/COPIAS FÍSICAS

1. Los documentos en papel que contengan Información Confidencial siempre deben colocarse en gabinetes o cajones cerrados con llave cuando no estén siendo utilizados. Dichos documentos no se pueden dejar en

[14] Dependiendo de la función laboral de cada quien, los miembros de la fuerza laboral de HAI tendrán diferentes niveles de interacción con la Información Confidencial. Algunos pueden trabajar directamente con información de participantes individuales, otros pueden trabajar con un conjunto de datos agregado que contiene información desidentificada. Es importante determinar el nivel de acceso de cada documento de funciones laborales en esta etapa temprana en la lista de actores previamente aprobados.
[15] Datos personales significa cualquier información relacionada con una persona física identificada o identificable (un 'interesado'). Una persona física identificable es aquella que puede ser identificada, directa o indirectamente. Para más información, ver Glosario de Términos.
[16] La información confidencial personal quiere decir cualquier información privada y que podría dañar a un individuo si se hace pública. Para ejemplos, ver Glosario de Términos.

espacio abierto en ningún momento (en estaciones de trabajo, residencia u otro espacio público, etc.), tanto dentro como por fuera del entorno de la oficina de HAI.

2. El almacenamiento no se considerará seguro a menos que haya una cerradura que funcione y que solo se pueda desbloquear con una llave.

ARCHIVOS/FORMULARIOS ELECTRÓNICOS

3. Guarde los documentos electrónicos en una carpeta debidamente restringida. Las preguntas y solicitudes sobre opciones seguras para guardar y compartir archivos deben dirigirse al departamento de TI.

- No guarde archivos electrónicos en las carpetas de *"Documentos"*, *"Escritorio"* en la unidad C:. Esto se aplica tanto a las computadoras portátiles como a las computadoras de escritorio de HAI. Los archivos guardados en C: se pueden borrar en cualquier momento, están expuestos a violación de datos y se perderán permanentemente.

- Cada empleado debe tener una unidad de red de HAI segura en su computadora portátil de HAI, así como una unidad I:.

- Dependiendo de su ubicación y nivel de autorización, tendrá acceso a una unidad compartida de HAI (unidad H:, O:, o S:).

- El almacenamiento de archivos basado en la nube (por ejemplo, Dropbox, iCloud, Google Drive, OneDrive, etc.) es conveniente, pero es vulnerable a ataques cibernéticos.

  La Información Confidencial (información comercial de HAI, datos personales o información confidencial personal de los participantes o miembros de la fuerza laboral) nunca debe almacenarse en proveedores comerciales en la nube no mantenidos por HAI.

III. PROTOCOLO DE TRANSFERENCIA DE INFORMACIÓN (PTI)

El intercambio de información es la etapa más crítica en el procesamiento de la información porque es donde ocurren las violaciones con mayor frecuencia. La violación de la información puede ocurrir con o sin el conocimiento de la persona, intencionalmente o por error. Es posible que las personas ni siquiera se den cuenta de que se divulgó una información sin la debida precaución y conciencia de la situación. Es por eso que es extremadamente importante establecer y seguir un conjunto de protocolos basados en los propósitos y el destinatario de la información compartida.

1. Prueba del mínimo necesario

Como regla base, cualquier intercambio de Información Confidencial, en forma verbal, electrónica o en papel, debe limitarse a la cantidad **mínima** de individuos y entidades **necesaria** para el correcto desempeño de las funciones de la organización. La Información Confidencial nunca debe compartirse por motivos de conveniencia. El intercambio de información debe realizarse según sea necesario.

2. ¿Quién puede compartir Información Confidencial?

Solo los miembros o afiliados autorizados de la fuerza laboral de HAI pueden compartir Información Confidencial.

- La autorización para *recolectar* o *acceder a* La Información Confidencial ***no*** otorga automáticamente a un individuo la autorización para compartir esa información.

- Los miembros de la fuerza laboral y afiliados de HAI que deseen compartir Información Confidencial deben tener: 1) sus nombres, cargos y niveles de acceso incluidos en la lista de "actores preaprobados"; o 2) un documento que acredite la autorización del supervisor del agente y del personal superior de HAI.

- La divulgación no autorizada de Información Confidencial (intencional o accidental) es una forma grave de violación; por lo tanto, los miembros de la fuerza laboral o afiliados de HAI que compartan Información Confidencial sin la debida autorización enfrentarán medidas disciplinarias.

- La actividad de recopilación de información primero debe pasar la prueba estándar del *mínimo necesario.* El agente debe preguntar si el intercambio de información es necesario para la operación de HAI y su misión de promover el bienestar de los participantes.

- El intercambio de información debe realizarse de una manera que minimice el riesgo, si lo hay, para la fuente de datos y/o el interesado. Cualquier actividad de recopilación de información que ocurra en una configuración de seguridad de riesgo medio o alto primero debe obtener la autorización del Jefe de Seguridad de HAI.

- El número de personas que comparten la información (por ejemplo, agrimensores, trabajadores sociales que completan la admisión, etc.) debe ser mínimo.

- La cantidad de información compartida debe ser mínima: solo comparta lo que debe compartirse. No comparta información periférica innecesaria haciendo preguntas no relacionadas, tomando notas sobre detalles no relacionados, tomando fotos de la casa del participante, etc.

3. Uso permitido: Implementación de programa

La implementación del programa es uno de los propósitos para los cuales se puede compartir Información Confidencial entre individuos. Al hacerlo, los miembros de la fuerza laboral y afiliados de HAI deben cumplir con la obligación de mantener los estándares de protección de datos de confidencialidad y seguridad.

- Las actividades de implementación del programa pueden incluir: prestación de servicios (alcance, admisión, reclutamiento, gestión de casos, seguimientos, etc.), monitoreo y evaluación (incluyendo informes internos) e informes de donantes, referenciación (interna o externa).

INTERCAMBIO CON OTROS MIEMBROS DE LA FUERZA LABORAL DE HAI

Ser miembro de la fuerza laboral de HAI ***no*** concede automáticamente el derecho de acceder a, divulgar o compartir Información Confidencial. Solo el personal del proyecto y el personal del programa cuya función laboral central requiere el intercambio de Información Confidencial puede hacerlo sin obtener una aprobación para cada ocasión.

- Para compartir Información Confidencial con cualquier otro miembro de la fuerza laboral de HAI, se debe establecer una de las siguientes condiciones:

  a) que el nombre, cargo y nivel de acceso del agente esté incluido en la lista de "actores preaprobados"[17]
  b) que el agente haya obtenido una constancia de autorización del supervisor del agente y del personal superior de HAI.

INTERCAMBIO CON AFILIADOS

Los afiliados incluyen personal a tiempo completo o parcial, voluntarios, y pasantes de organizaciones receptoras de subvenciones. También incluye consultores, asesores o contratistas asociados con proyectos de HAI a través de un acuerdo o contrato. Solo las personas cuyo deber laboral central requiere acceder y compartir Información Confidencial pueden hacerlo sin obtener una aprobación para cada ocasión.

- En general, los acuerdos y contratos sub-adjudicados deberán incluir una cláusula de no divulgación. Después de firmar los acuerdos de subcontratación, los afiliados en la organización subcontratada que puedan estar manejando cualquier Información Confidencial deben leer y firmar el Formulario de Reconocimiento de Confidencialidad y Seguridad de HAI. El documento original firmado se guardará para registro de HAI, y se podrá proporcionar una copia en papel al afiliado si así lo solicita.

- Para que los afiliados individuales obtengan acceso a Información Confidencial, debe cumplirse una de las siguientes:

  a) La lista de "actores previamente aprobados", vinculada a la información solicitada, que contiene el nombre, el cargo y el nivel de acceso del agente; o
  b) Una autorización apropiada del supervisor del agente y del personal superior de HAI.

[17] Dependiendo del cargo de cada quien, los miembros de la fuerza laboral de HAI tendrán diferentes niveles de interacción con la Información Confidencial. Algunos pueden trabajar directamente con información de participantes individuales, otros pueden trabajar con un conjunto de datos agregado que contiene información desidentificada. Es importante determinar el nivel de acceso de cada documento de funciones laborales en esta etapa temprana en la lista de actores previamente aprobados.

INTERCAMBIO CON SUBCONTRATISTAS

Los subcontratistas son personas o entidades a quienes un afiliado delega una función, actividad o servicio, en calidad diferente a la de miembros de la fuerza laboral de dicho afiliado. Los subcontratistas son diferentes de los afiliados en que no celebran un contrato o un acuerdo con HAI; sin embargo, desempeñan funciones centrales para, o en apoyo de, las actividades del proyecto del programa de HAI.

- Dado que no existe un contrato o acuerdo con HAI, los gerentes de proyecto deben asegurarse de que los subcontratistas individuales lean y firmen el Formulario de Reconocimiento de Confidencialidad y Seguridad. El documento original firmado se guardará para registro de HAI, y se podrá proporcionar una copia en papel al afiliado si así lo solicita.

- La firma del Formulario de Reconocimiento de Confidencialidad y Seguridad se aplica a cualquier subcontratista individual que maneje directamente Información Confidencial.

- Esto también se aplica a los subcontratistas cuyo trabajo puede no manejar directamente la Información Confidencial y, sin embargo, cuya función, actividad o servicio se produce en entornos donde la Información Confidencial está en riesgo de ser escuchada o divulgada a escondidas[18]:

    a. donde se recopila Información Confidencial (por ejemplo, campamentos de desplazados internos donde los encuestadores recopilan información);
    b. donde se discuta la Información Confidencial (por ejemplo, sala de consulta, área de recepción en centros de tratamiento médico);
    c. donde se divulgue Información Confidencial en entornos restringidos para una función de trabajo central (por ejemplo, oficina de la persona que ingresa los datos, trabajador social o gestor de casos); o
    d. donde se almacena la Información Confidencial (por ejemplo, la oficina de HAI o la oficina de las organizaciones de subcontratadas donde se almacenan los archivos de casos).

4. Otros propósitos de HAI

Puede haber ocasiones en que se solicite Información Confidencial para fines de HAI que no esté directamente vinculada a la implementación del programa. Los ejemplos pueden incluir: historias de participantes para divulgación, promoción de servicios, comunicaciones o relaciones externas.

En todas las ocasiones, la Información Confidencial debe manejarse con precaución y se aplica el principio del mínimo necesario: la Información Confidencial compartida para tales fines debe ser la mínima necesaria para la operación de HAI.

Es responsabilidad del agente completar los siguientes procedimientos *antes* de iniciar cualquier actividad de recopilación de información:

Paso 1: El agente proporciona justificación de por qué dicha actividad de intercambio de información es necesaria para la operación/programa de HAI. El agente debe presentar una declaración por escrito:

a. para qué se utilizará la información una vez compartida (por ejemplo, objetivo de la actividad);
b. cómo se compartirá la información, por ejemplo, frecuencia de uso compartido, tipo de medio (electrónico, papel), uso de correo electrónico, correo, fax, etc.
c. cómo la información, una vez compartida para el propósito de HAI, será retroalimentada a HAI;
d. si los beneficios superan los riesgos (tanto a nivel individual como organizacional); y

[18] Para obtener una definición más detallada de "escuchas", consulte el Glosario de Términos.

e. una garantía escrita del agente de que se adhiere a la política de HAI durante la recopilación de datos y que no recopilará, accederá a o compartirá la Información Confidencial para ningún propósito más allá de lo autorizado.

Paso 2: El agente presenta la declaración a 1) su supervisor, 2) un miembro del personal directivo superior del país donde se realizará la recopilación de información, y 3) el gerente del proyecto correspondiente.

c. Debe discutir la declaración escrita que justifica la recolección.
d. Discutir los beneficios y riesgos para las personas involucradas y para HAI. Los puntos focales directos deben brindar insumos sobre esta discusión (por ejemplo, trabajadores sociales, personal que interactúa directamente con los participantes).

Paso 3: Una vez que todos estén de acuerdo en que los beneficios superan los riesgos, se puede contactar a la fuente de datos.

Obtención del consentimiento de los participantes de HAI: el trabajador social designado y el gerente del proyecto (si corresponde) deben primero aprobar la actividad de intercambio de información. Para los participantes que pueden tener desafíos adicionales para comprender el consentimiento debido a su edad, estado de discapacidad y otros factores de vulnerabilidad, también debe estar presente un cuidador que pueda abogar por el participante.

Paso 4: Al contactar con la fuente de datos, el agente debe primero explicar el objetivo del intercambio de información. Indicar claramente qué información están buscando los agentes. Si la fuente de datos expresa interés en proporcionar la información, puede darse inicio al proceso de consentimiento informado.

Nota: asegúrese de que la fuente de datos sea capaz de dar su consentimiento. Muchos factores pueden invalidar el consentimiento (por ejemplo, la edad, condición de discapacidad, dinámica de poder, etc.) dependiendo de los requisitos legales locales. Asegúrese de que la fuente de datos pueda comunicarse libremente con los agentes; de lo contrario, se debe proporcionar un traductor para explicar las condiciones de consentimiento en la lengua materna de la fuente de datos.

Paso 5: Revisar el formulario de consentimiento estándar de HAI completo. Antes de solicitar el consentimiento después de explicar el contenido, el facilitador debe preguntar si la fuente de datos potencial tiene alguna pregunta. Una vez que la fuente de datos expresa que comprende completamente la condición del consentimiento, los facilitadores pueden solicitar formalmente su consentimiento y firma/huella digital en el formulario de consentimiento de HAI.

Nota: La coerción, explícita o implícita, o las falsas promesas hechas en cualquier etapa del proceso de consentimiento invalidan el consentimiento otorgado por el participante.

Paso 6: Los agentes deben proporcionar una copia del formulario de consentimiento firmado a 1) la fuente de datos; y 2) al trabajador social. Los agentes también deben proporcionar su información de contacto para cualquier pregunta que pueda surgir en el futuro.

Nota: Para el caso de Colombia, los propósitos con los que se recopilan, recolectan, almacenan y en general, se les da Tratamiento a los Datos Personales, se encuentran definidos en el CAPÍTULO 6: POLÍTICA ESPECÍFICA DEL PAÍS.

5. Propósitos no relacionados con HAI

Las entidades externas pueden solicitar a los miembros de la fuerza laboral y afiliados de HAI que compartan una información que es, o puede ser, confidencial. Ejemplos de entidades de terceros son: autoridades gubernamentales, fuerzas del orden, investigadores, periodistas u otras organizaciones de la sociedad civil, etc.

Como regla de referencia, HAI debe evitar compartir cualquier información con personas externas a HAI o de entidades de terceros no aprobadas. El intercambio de información, por muy inocuo que sea el propósito, expone la Información Confidencial a riesgos de divulgación por error humano y puede llamar la atención no deseada a los participantes, las comunidades, los proyectos de HAI y los miembros de su fuerza laboral y afiliados.

Se requiere autorización en cualquier intercambio de información externa con entidades de terceros. Para obtener instrucciones detalladas, tenga en cuenta:

- Las solicitudes de medios serán evaluadas caso por caso por el Director de Relaciones Externas/Comunicación.

- Las solicitudes relacionadas con la investigación serán evaluadas caso por caso por el Director de Investigación/Director Asociado de Investigación, Monitoreo y Evaluación.

Nota: Para el caso de Colombia, los propósitos con los que se recopilan, recolectan, almacenan y en general, se les da Tratamiento a los Datos Personales, se encuentran definidos en el CAPÍTULO 6: POLÍTICA ESPECÍFICA DEL PAÍS.

6. Método seguro de intercambio de información

Una vez obtenida la autorización para compartir Información Confidencial, los miembros de la fuerza laboral y afiliados de HAI deben utilizar el siguiente método de transferencia para enviar cualquier archivo electrónico o copia en papel que contenga Información Confidencial.

ARCHIVOS ELECTRÓNICOS COMPARTIDOS MEDIANTE CORREO ELECTRÓNICO

- Marque el archivo electrónico como confidencial.

  Los archivos electrónicos que contienen Información Confidencial deben tener etiquetas explícitas que indiquen su naturaleza confidencial. Use cualquiera de los siguientes métodos:

  a) Coloque una marca de agua de identificación "CONFIDENCIAL".

  b) Inserte texto en el encabezado o pie de página del documento señalando que es "confidencial", "no para su distribución" u otra marca que lo designe como confidencial.

- Los archivos electrónicos compartidos por correo electrónico deben estar protegidos con contraseña.

Nota importante: las contraseñas para archivos adjuntos nunca deben compartirse dentro del correo electrónico al que están adjuntos.

PAPEL/IMPRESO/COPIAS FÍSICAS

- Al distribuir documentos físicos de carácter confidencial para una reunión o discusión presencial, asegúrese de que los artículos estén marcados como confidenciales, como se indicó anteriormente, y reúna todas las copias al final de la reunión sin dejar ninguna a disposición.

- Durante las reuniones, informe a los destinatarios de la información que dicha información es de propiedad exclusiva y/o confidencial y no debe compartirse con otras personas que no necesitan saber.

- En las comunicaciones electrónicas a destinatarios autorizados, se puede insertar el siguiente descargo de responsabilidad en el documento o en la comunicación por correo electrónico:

  CONFIDENCIAL
  Este documento contiene Información Confidencial propiedad de Heartland Alliance International. El acceso y uso de esta información está estrictamente limitado y controlado por la Compañía. Este documento no puede ser copiado, distribuido o de otra manera divulgado por fuera de Heartland Alliance International, excepto bajo las precauciones apropiadas para mantener su confidencialidad, y no puede usarse de ninguna manera que no esté expresamente autorizada por Heartland Alliance International.

Las preguntas adicionales sobre si marcar o designar documentos u otra información como confidencial, o de otra manera, deben dirigirse al área de Operaciones en Colombia.

Los documentos deben almacenarse y archivarse en un lugar adecuado en cuanto a dimensiones y acondicionamiento para proteger su integridad física y para que sean de fácil acceso.
Cada carpeta / archivo debe estar debidamente etiquetada con la información de año, nombre del proyecto y contenido.

La documentación se clasificará, ordenará y archivará de acuerdo a los resultados esperados y a las actividades a las que hace referencia. Todos los documentos de un mismo proyecto deberán almacenarse en un folio con divisores para mantener la información ordenada.
El gerente de proyecto deberá definir un plan de archivo para organizar, monitorear y sistematizar la documentación justificativa técnica durante la vida del proyecto. Los referentes(s) técnico(s) del equipo de coordinación involucrados en el proyecto deberán validar el plan de archivo.

IV. PROTOCOLO DE RETENCIÓN DE DATOS

Eliminar, destruir o deshacerse de forma permanente de todas las copias en papel y electrónicas de la Información Confidencial una vez que se haya cumplido su propósito.

Dependiendo del donante y del proyecto, se establece el tiempo en el cual se debe mantener el archivo físico y digital de los documentos soporte de las actividades realizadas. Se debe asegurar que tanto los documentos como los archivos digitales estén protegidos durante este tiempo de todos los posibles riesgos, según lo descrito en este manual. Una vez cumplido el plazo establecido y realizadas las actividades de auditoría necesarias, las copias deben destruirse y disponerse de la manera que establece el manual.

1. Regla general

Triturar documentos inmediatamente después de la transcripción, uso o período de almacenamiento requerido.

CAPÍTULO 4: PROTOCOLO DE CYBERSEGURIDAD

Alcance: Esta política se aplica a todos los miembros de la fuerza laboral internacional de Heartland Alliance y sus afiliados que residen o visitan las oficinas de HAI fuera de los Estados Unidos.

HAI debe proteger la Información Confidencial de cualquier uso o divulgación intencional o no intencional. Para proteger a todos los participantes, miembros de la fuerza laboral, la reputación y activos de la organización, se deben implementar los siguientes protocolos para mitigar el riesgo de seguridad. Las siguientes secciones sobre seguridad de la información, ciberseguridad, seguridad de instalaciones y dispositivos móviles representan **la práctica del estándar mínimo para todas las oficinas de país de HAI**. Los siguientes protocolos son específicos para los miembros de la fuerza laboral o afiliados de HAI que residen o visitan las oficinas del programa fuera de los Estados Unidos.

I. PROTOCOLO DE SEGURIDAD INFORMÁTICA

- Toda la fuerza laboral y afiliados de HAI, incluidos los consultores, el personal de organizaciones asociadas, voluntarios o pasantes, que acceden a la Información Confidencial deben firmar el formulario de Reconocimiento de Confidencialidad y Privacidad de HAI.

- Se aplican normas más estrictas a los afiliados de HAI, incluidos consultores, personal de organizaciones asociadas, voluntarios o pasantes.

    - Los afiliados no pueden recopilar, transmitir o almacenar información escrita en ninguna entidad gubernamental o centro de detención.

    - Los afiliados no pueden acceder a la Información Confidencial a menos que se mencione directamente en la descripción del trabajo. Los afiliados no pueden llevar ningún archivo escrito o electrónico que contenga la operación de HAI (es decir, documentos internos) e información del proyecto de HAI.

    - Los afiliados no pueden usar su dispositivo móvil privado para recopilar, almacenar o compartir Información Confidencial en ninguna circunstancia.

- Cuando trabaje con Información Confidencial en su computadora portátil/computadora/otros dispositivos móviles, nunca se vaya sin antes bloquear el dispositivo con la contraseña que solo usted conoce. Puede bloquear fácilmente su computadora portátil/computadora haciendo clic en estas teclas en su teclado:

    - Ctrl + Alt + Eliminar; o

    - Ventana + L

- El departamento de TI debe revocar el acceso de los empleados desvinculados a la red en un plazo de 3 días.

- Los nombres y afiliaciones de los participantes se mantienen estrictamente confidenciales, excepto cuando sea necesario para informar al donante y para el pago de viáticos o reembolsos de viaje.

- HAI no permite que se tomen fotografías de los participantes y no publica información sobre el proyecto, incluso en medios impresos o sociales.

- Los dispositivos robados con Información Confidencial o de los participantes deben informarse en RMIS de inmediato. Si no se informan posibles infracciones de seguridad de la información, el personal puede ser suspendido o desvinculado.

- Se debe realizar una evaluación de riesgos para cada posible violación de seguridad. Si el equipo de seguridad y del país cree que la información de los participantes puede verse comprometida y aumentar los riesgos que representa para los participantes, estos serán notificados de inmediato. Consulte la siguiente sección sobre infracciones de seguridad de la información para obtener más información.

- Los miembros del personal que trabajan en proyectos altamente sensibles deben someterse a un curso de actualización de seguridad cibernética ofrecido por el departamento de TI de HAI. Los proyectos altamente sensibles también pueden tener un programa de información y ciberseguridad específico.

- El departamento de TI de HAI puede querer agregar algunas secciones sobre protocolos específicos de uso de Internet; esto está en línea con uno de los comentarios que he dado a continuación en relación con los protocolos de seguridad cibernética

- Uno de los protocolos podría ser cambiar la contraseña de Internet. En Iraq, el personal que abandonó HAI en noviembre, febrero de 2017 todavía puede conectarse para visitar la oficina ahora.

- Todos los participantes reciben una sesión informativa sobre ciberseguridad en su orientación donde revisan las medidas estándar de ciberseguridad y reciben orientación sobre prácticas seguras para la comunicación virtual.

- Los miembros del personal utilizan las aplicaciones designadas de teléfono y correo electrónico para comunicarse con los participantes. Estas aplicaciones se seleccionan en función de una evaluación de riesgos de información y ciberseguridad.

- Deber de cuidado al no informar a los usuarios que su información personal será utilizada y obtener un consentimiento válido para usar la información personal.

- Se utilizarán VPN en países con amenazas de ciberseguridad de alto riesgo. Los participantes también pueden recibir capacitación sobre protocolos VPN básicos y aplicaciones de seguridad aceptables que se utilizarán para la comunicación.

- HAI garantiza que no se codificará información sobre el origen del documento o las direcciones IP en los materiales de capacitación, planes de estudio o encuestas que se producen como parte del proyecto.

II. CONTROL DE ACCESO FÍSICO

La Información Confidencial a menudo se almacena en papel y/o en formato electrónico y se deja en las oficinas. Los incidentes de incumplimiento, especialmente las infracciones accidentales y no intencionales, ocurren con mayor frecuencia en tales oficinas. Para evitar dichos eventos, se espera que las oficinas de HAI en los países cumplan con los siguientes protocolos:

Lo siguiente se aplica a las instalaciones/sitios donde se almacena la Información Confidencial:

1. Entrada (puertas) a las instalaciones

- Todas las puertas exteriores no públicas (como las puertas solo para empleados) y las puertas que conducen a áreas donde reside la Información Confidencial deben permanecer cerradas en todo momento.

- Es responsabilidad de cada miembro de la fuerza laboral asegurarse de que las puertas de ingreso o salida están completamente cerradas antes de partir. Si el mecanismo de cierre o ajuste de la puerta no funciona, los miembros de la fuerza laboral deben notificar al gerente de la instalación.

2. Control de acceso a la oficina

- Solo los miembros autorizados de la fuerza laboral deben recibir los niveles de acceso a las instalaciones y/o al sitio de trabajo apropiados para su rol laboral.

- Formato de identificación estándar uniforme para los miembros de la fuerza laboral que trabajan en la misma oficina en el país.

- Autorizaciones definidas basadas en la necesidad programática, requisitos de seguridad obligatorios especiales y seguridad del personal

- Documentación para aprobación de autorizaciones aprobadas

- Sistema para deshabilitar/recuperar/destruir tarjetas cuando los miembros de la fuerza laboral dejan el empleo

3. Control de acceso de visitantes

- Todos los visitantes, incluidos los participantes, deben ser escoltados y monitoreados. Cada instalación implementará procedimientos que varían según la estructura, el tipo de visitantes y el lugar donde se almacena la Información Confidencial.

- Los visitantes no deben dejarse desatendidos, excepto en las áreas públicas de espera.

- Los visitantes pueden firmar un registro de visitantes que incluye el nombre del visitante y la fecha y hora de entrada y salida. Si se utiliza un registro de visitantes para los participantes en el entorno médico, su información se ocultará una vez que se haya registrado para proteger la privacidad.

- Si el visitante es un participante, el personal puede registrarlo a través de su ingreso en el registro médico electrónico en lugar de un registro de visitante

- Solo los visitantes que tengan una justificación comercial serán admitidos en áreas en las que reside Información Confidencial

4. Control de acceso al almacenamiento

- Armarios/gabinetes en las instalaciones: Las unidades de almacenamiento que almacenan medios tangibles (papel, cinta de video, CD, unidad USB) que almacenan Información Confidencial se deben asegurar con un candado siempre que el armario esté desocupado o no esté en uso. Quien administre el gabinete que contiene Información Confidencial debe mantener un registro de las personas que solicitan acceso a dicho gabinete.

- Llaves metálicas/duras: Las instalaciones que usan llaves metálicas/duras deben cambiar las cerraduras cuando las llaves se pierden o no son devueltas.

Para obtener una lista detallada de las responsabilidades delegadas al gerente, miembro del personal y jefe de las instalaciones, consulte la política de HA en Controles de acceso a las instalaciones.

III. USO DE DISPOSITIVOS MÓVILES

Los dispositivos móviles, por naturaleza, son muy vulnerables al robo, pérdida, piratería y otras formas de violación que ponen en peligro el contenido almacenado en cuestión de segundos. Con los ataques cibernéticos cada vez más accesibles y generalizados, los dispositivos móviles son el objetivo más fácil para cualquier persona (incluso los piratas informáticos no profesionales) que buscan violar la seguridad de la información y causar daños físicos, psicológicos, financieros y de reputación a un individuo u organización.

Los dispositivos móviles (computadoras portátiles, teléfonos inteligentes, tabletas, unidades flash USB, tarjetas de memoria) pueden exponer a los miembros de la fuerza laboral, afiliados y participantes a un mayor peligro de convertirse en víctimas de delitos. Si el dispositivo móvil lleva alguna información de naturaleza sensible: Información personal, Información confidencial personal (ICP)e Información Privilegiada- el riesgo de daño se vuelve exponencialmente mayor. Para la seguridad de los miembros de la fuerza laboral, afiliados y participantes, HAI adopta la siguiente política con respecto al uso del dispositivo móvil durante la operación de HAI:

1. Dispositivos móviles emitidos por HAI

Administración: Para cada oficina en el país, un oficial dedicado (idealmente un funcionario de TI) supervisa la implementación del protocolo y el mantenimiento de los dispositivos móviles de HAI. Cada oficina también debe adquirir tantas computadoras portátiles encriptadas como sea financieramente posible. Los nuevos programas deberían presupuestar nuevas computadoras portátiles encriptadas, especialmente para programas con un mandato de alto riesgo.

Almacenamiento: En todo momento, todos los dispositivos móviles de HAI deben almacenarse en lugares seguros (por ejemplo, armarios cerrados, cajuela de automóvil, etc.) fuera de la vista pública, independientemente de la ubicación del usuario (por ejemplo, oficinas, sitios de proyecto, en tránsito, etc.).

Contraseña: En todo momento, todos los dispositivos móviles de HAI (computadoras portátiles, teléfonos inteligentes, tabletas, unidades flash USB, tarjetas de memoria) deben estar protegidos con contraseña. Estas contraseñas no deben compartirse. Las contraseñas deben cambiarse cada vez que hay un nuevo usuario.

> ***Nota importante:*** *Nunca abandone el dispositivo sin bloquearlo con una contraseña. Puede bloquear fácilmente su computadora portátil/computadora haciendo clic en estas teclas en su teclado: [Ctrl + Alt + Supr] o [Ventana + L]*

Información Confidencial: HAI desaconseja firmemente que sus miembros de personal y afiliados creen, almacenen o compartan cualquier información relacionada con el proyecto que pueda tener una naturaleza personal, confidencial o reservada. Llevar Información Confidencial en cualquier dispositivo móvil puede poner en peligro la seguridad física y psicológica de los miembros de la fuerza laboral, afiliados y participantes. También puede causar daños financieros y de reputación a la organización.

Si esto se vuelve inevitable, no hay alternativas, y el mandato de HAI requiere que la Información Confidencial se almacene en un dispositivo móvil emitido por HAI *temporalmente*, se aplicarán las siguientes reglas:

- los archivos electrónicos que contienen Información Confidencial deben estar encriptados con una contraseña;
- El personal de HAI debe mantener el dispositivo móvil cerca de ellos, fuera de la vista del público, y almacenar los dispositivos móviles en un gabinete cerrado o en la cajuela de un vehículo cuando se deja desatendido;
- tan pronto como termine la tarea, completar los siguientes pasos lo antes posible:

Paso 1: Primero, guarde el archivo electrónico que contiene Información Confidencial en un lugar seguro (por ejemplo, copias en papel almacenadas en gabinetes con cerradura, servidor seguro de HAI);

Paso 2: Elimine el archivo que contiene Información Confidencial del dispositivo móvil;

Paso 3: Elimine cualquier otro archivo que pueda no ser confidencial pero que aún esté relacionado con la asignación (por ejemplo, notas que contengan contraseñas para el archivo encriptado, números de teléfono de personas, dirección de ubicación, etc.) del dispositivo móvil;

Paso 4: Devuelva el dispositivo móvil a la persona que lo emitió (por ejemplo, oficina, gerente de operaciones). Si la persona no está disponible de inmediato, guarde el dispositivo en un armario con cerradura y devuélvalo lo antes posible.

2. Dispositivos móviles personales

- HAI *prohíbe rotundamente* a los miembros de su personal y a sus afiliados utilizar su dispositivo móvil personal/privado, incluso temporalmente, para crear, almacenar y compartir cualquier Información Confidencial. Esto incluye comunicarse con los participantes.

- HAI desaconseja firmemente el uso de dispositivos móviles privados que no sean de HAI para llevar a cabo cualquier propósito comercial de HAI, incluida la discusión de negocios de HAI con colegas. Sin embargo, hay excepciones:

  - en caso de emergencias, según lo determine el Director de País o el Subdirector de País;

  - si no hay un dispositivo móvil de HAI disponible y no hay otras alternativas a la comunicación. En tal caso, se aplican las siguientes reglas:

    - Cualquier dispositivo personal utilizado para asuntos de HAI debe estar protegido con contraseña en todo momento, independientemente de su ubicación.

    - Cualquier dispositivo personal utilizado para el correo electrónico y el calendario de Microsoft Outlook debe estar protegido con Citrix.

CAPÍTULO 5: INFORME & RESPUESTA A INCIDENTES DE VIOLACIÓN

Un incidente de violación se refiere a un intento o violación exitosa de Información Confidencial que implica la divulgación o difusión de dicha información que no cumple con las políticas internas. Los ejemplos incluyen el robo o la pérdida de productos electrónicos que almacenan información identificable, la eliminación inadecuada de los registros de los participantes o empleados, o el acceso o divulgación no autorizados (es decir, enviar un fax a un número incorrecto o piratear información). Los incidentes de violación pueden justificar una respuesta a la crisis si la seguridad o activos del miembro del personal de HAI están amenazados. Para obtener una definición más detallada, ejemplos de incidentes de seguridad y responsabilidades en el plan de respuesta, consulte la política de HA en *Informes y respuesta a incidentes de seguridad de la información*.

I. ¿QUE ES UN INCIDENTE DE VIOLACIÓN?

Un incidente de violación es el evento de destrucción accidental o ilegal, pérdida, alteración, divulgación no autorizada o acceso a, Información Confidencial—Incluida información relacionada con HAI. Cualquier incidente o evento intencional o no intencional, sospechado o real que afecte, amenace o viole la confidencialidad, integridad o disponibilidad de la Información Confidencial se considera un incidente de violación. Se requiere que los miembros de la fuerza laboral de HAI presenten de inmediato un Informe de incidentes de posible violación de Información Confidencial a RMIS según se indica en la siguiente sección.

Se debe realizar una evaluación de riesgos para cada posible violación de seguridad. Si el equipo de seguridad y del país cree que la información de los participantes puede verse comprometida y aumentar los riesgos que representa para los participantes, estos serán notificados de inmediato. Consulte la siguiente sección sobre infracciones de seguridad de la información para obtener más información.

1. Tipos comunes de incidentes de violación

- *Correos electrónicos/fax/copia en papel con Información Confidencial enviada accidentalmente a la persona equivocada.*

- *Los dispositivos electrónicos que contienen Información Confidencial se extravían, son robados o confiscados por fuerzas de seguridad o por la policía.* Informe si se pierden/hurtan los siguientes dispositivos electrónicos:

    - Dispositivo de propiedad personal que contiene información relacionada con HAI.
    - Dispositivos móviles emitidos por HAI (teléfonos móviles, computadoras portátiles, tabletas, CD, unidad USB, etc.)
    - Computadoras de escritorio en la oficina de HAI.
    - Para dispositivos electrónicos perdidos/robados, debe enviar un correo electrónico al departamento de TI (helpdesk@heartlandalliance.org) e informar que su dispositivo se perdió/fue robado. Después de enviar este correo electrónico, debe enviar el informe RMIS.

- *Los documentos físicos que contienen Información Confidencial se extravían, son robados o confiscados por fuerzas de seguridad o por la policía.*

- *Incidentes de entidad:* acceso no autorizado a la oficina física de HAI (o sus afiliados) que podría comprometer la Información Confidencial. Ejemplos incluyen:

- Persona no autorizada encontrada en una ubicación de Heartland donde se almacena Información Confidencial, que tiene el potencial de haber sido obtenida por dicha persona no autorizada
- El allanamiento físico de la oficina que puede haber resultado en la exposición de la Información Confidencial

- *Eventos de seguridad de red:* La sospecha o amenaza real de un virus, malware, contraseña comprometida o una violación del sistema de cualquier computadora o dispositivo que tenga acceso a Información Confidencial.

  - Códigos maliciosos como virus, gusanos, troyanos u otros códigos que amenacen la red o dispositivos de HAI en los que se almacena Información Confidencial
  - Suplantación de identidad (phishing) u otros ataques cibernéticos que pueden haber comprometido la red o los dispositivos de HAI en los que se almacena Información Confidencial
  - Intrusiones exitosas que pueden comprometer la red o sus datos
  - Incidentes de fraude informático, ataques de denegación de servicio, penetración o alteración del sistema
  - Uso no autorizado, alteración o destrucción de datos, software o equipos.
  - Uso de dispositivos informáticos de Heartland Alliance para cometer actos ilegales

  - Para estos incidentes de ciberseguridad, debe hacer lo siguiente: 1) enviar un correo electrónico al departamento de TI (helpdesk@heartlandalliance.org) e informar que su dispositivo se perdió/fue robado; 2) enviar el informe RMIS.

II. PLAN DE RESPUESTA A INCIDENTES DE VIOLACIÓN

Los informes de incidentes de RMIS deben enviarse cada vez que los miembros del personal *sospechan* que existe una violación. No se requiere prueba de la existencia real de una violación para presentar el informe.

Aviso importante: Los miembros del personal no reportarán los dispositivos robados a las autoridades locales. Algunos dispositivos pueden contener información que podría poner en riesgo a los participantes si son descubiertos por las autoridades.[19]

1. Procedimiento estándar de respuesta

1. Descubrimiento de posible incidente de violación.

2. Debe presentarse un informe de "Violación potencial de Información Confidencial" en RMIS dentro de un plazo de 24 horas. Los miembros de la fuerza laboral de HAI pueden acceder al sistema de informes de RMIS visitando el Sitio de intranet de Heartland Alliance , luego haciendo clic en "*RMIS* " en el lado derecho de la página de inicio. Lo verá cerca de la parte inferior de *"Enlaces de la página principal".*

3. Para los tipos de incidentes, seleccione ambos *"Incumplimiento potencial de Información Confidencial protegida o de salud"* y *"Seguridad o prevención"*.

4. En general, se debe recopilar e informar el siguiente contenido mínimo de información:

   - *Una descripción de la naturaleza de la violación: detalla los elementos tecnológicos que se tomaron, sus números de serie, la información que contenían y la información de contacto de los miembros del personal que poseían los elementos;*
   - *El nombre y los detalles de contacto del funcionario de protección de datos u otro punto de contacto;*
   - *Una descripción de las posibles consecuencias de la violación; y*
   - *Una descripción de las medidas tomadas o propuestas a ser tomadas por el controlador para abordar la violación, incluidas, cuando corresponda, medidas para mitigar sus posibles efectos adversos.*

5. Una vez que se haya informado un incidente de violación, el equipo de seguridad y TI realizará una evaluación de riesgos. Si una crisis es inminente, el Director Ejecutivo de HAI reunirá al Equipo de Gestión de Crisis para responder al incidente.

6. Si la información del participante se vio comprometida y si la información comprometida representa un riesgo para el participante, se le notificará de inmediato.

7. El equipo de TI borrará de forma remota cualquier dispositivo de HAI cifrado y cuentas de correo electrónico comprometidas.

[19] Esta política contradice la política establecida en el manual de HA, que requiere que los miembros del personal denuncien los dispositivos robados a las autoridades de inmediato. Sin embargo, en el contexto operativo global de HAI, esta es una práctica que podría ser perjudicial para la seguridad de los miembros del personal y los participantes.

2. Notificación de Violación

Si se cree que la violación de la información pondrá en peligro a las personas, HAI notificará a esas personas lo antes posible. El formato de notificación de violación dependerá de la situación y el país de origen. Ver **Directrices de privacidad específicas del país** para más información específica del país.

Notificación de violación de información personal y respuesta a incidentes

CAPÍTULO 6: POLÍTICA ESPECÍFICA DEL PAÍS

COLOMBIA

En Colombia, la Ley de Protección de Datos Personales reconoce y protege el derecho de todas las personas a conocer y actualizar la información que hayan compartido, ya sea en base de datos o archivos, que pudiesen ser tratados. **Datos personales** son todos aquellos datos relacionados con la identificación de una persona, como el documento de identidad, lugar y fecha de nacimiento, estado civil, edad, lugar de residencia, trayectoria laboral o académica. Es importante diferencia el tipo de datos que existen bajo la ley colombiana:

a. **Datos públicos**: los datos que la Constitución Política determina como públicos, así como aquellos datos que no sean caracterizados como privados o semiprivados.
b. **Datos semiprivados**: datos que por su naturaleza no se caracterizan como públicos ni datos reservados y cuya divulgación puede interesar a un grupo de personas.
c. **Datos privados**: aquellos datos que por su naturaleza íntima sólo le son importantes al titular de los datos.
d. **Datos sensibles**: aquellos datos que afectan la intimidad del titular y cuyo uso indebido puede generar su discriminación. Por ejemplo, el estado salud de la persona, sus características físicas, ideología política, vida sexual y los datos biométricos.

Es importante destacar la diferencia entre transferencia de datos y la transmisión de datos. La **transferencia de datos** tiene lugar cuando es responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país. La **transmisión de datos** es el tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Acceder a la política de privacidad global en esta liga: https://www.heartlandalliance.org/about/privacy-policy/

I. REQUERIMIENTOS LOCALES DE PRIVACIDAD

Una lista detallada de los requerimientos de privacidad está disponible en la unidad O:. O:\10. Seguridad y cobertura\11. Seguridad de la información o a solicitud

A continuación, se muestra un resumen de las leyes de privacidad aplicables a cada uno de los países en que opera HAI.

PAÍS	LEY DE PRIVACIDAD	A DESTACAR
COLOMBIA	*Constitución Política de Colombia*	El artículo 15 establece que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección,

		tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
	Ley Nacional/Federal, Ley No. 1581	Contiene el marco general de la protección de datos personales en Colombia. Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información consagrada en el artículo 20 de la misma.
	Recolección de datos personales (Ley 1581 del 2012, artículo 4)	La recolección de estos datos debe limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente. Salvo en los casos expresamente previstos en la Ley, no se podrán recolectar datos personales sin autorización del Titular. Los responsables de la recolección de datos, deben proveer una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso.
	Autorización de datos personales (Ley 1581 del 2012, artículo 5 y 6)	El responsable del tratamiento de los datos personales, deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titula para el tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del tratamiento para las cuales se obtiene el consentimiento. Para el tratamiento de los datos sensibles, se le debe informar al titular que 1) por tratarse de datos sensibles, no está obligado a autorizar su Tratamiento, e 2) informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de datos personal, cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad del tratamiento, así como obtener su consentimiento expreso.
	Modo para obtener la autorización de datos (Ley 1581 del 2012, artículo 7)	Los responsables del tratamiento de datos personales establecerán mecanismos para obtener la autorización de los Titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 del presente decreto, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al titular su manifestación automatizada. Se entenderá que; la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca. Una vez que se obtenga la autorización, el responsable deberá guardar la prueba de la autorización.

	Revocación de la autorización y supresión de datos (Ley 1581 del 2012, artículo 9)	Los titulares de los datos pueden solicitar en todo momento la supresión de datos personales y/o revocar la autorización otorgada para el tratamiento de los mismos. Esta solicitud no procede cuando procede cuando el titular tenga un deber legal o contractual de permanecer en la base de datos. El responsable de los datos debe ofrecer mecanismos de revocación (gratuitos) y de fácil acceso para presentar la solicitud de supresión de datos.
	Políticas de tratamiento de datos (Ley 1581 del 2012, artículos 13 - 16)	Los responsables del tratamiento de datos deben desarrollar políticas para el tratamiento de los datos personales y velar porque los encargados del tratamiento cumplan con las mismas. En caso de no poner a disposición del titular las políticas del tratamiento de la información, entonces se deberá incluir un aviso de privacidad sobre la existencia de tales políticas y la forma de acceder a las mismas. En caso de que se recolecten casos sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

II. POLÍTICA DE TRATAMIENTO DE DATOS EN COLOMBIA

1. Datos Personales que recolectamos y tratamos.

Dependiendo del tipo de relación o vinculación que el Titular pueda tener con HAI, los Datos Personales que recolectamos y tratamos pueden ser uno o más de los siguientes:

- Su nombre,
- edad,
- el número de su documento de identificación o cédula de ciudadanía,
- su dirección de correo electrónico,
- su dirección IP,
- su lugar de residencia,
- su número de teléfono,
- sus nombres de usuario de Twitter y/o Facebook o de sus otras redes sociales,
- su ubicación geográfica,
- su nacionalidad y su lugar de domicilio,

2. Tratamiento al que estarán sujetos sus Datos Personales.

Los Datos Personales que Usted nos proporciona y cualquier otro al que tengamos acceso por cualquier fuente, incluidos los provenientes de terceros con quienes tenemos relaciones comerciales y/o contractuales, estarán sujetos a los siguientes tratamientos por parte de HAI, según el tipo de Dato Personal al que se refiere el tratamiento y dependiendo del tipo de relación o vinculación que tenga el Titular con HAI:

- Contactar a los participantes o Titulares para ofrecer los servicios, confirmar citas, proveer servicios, solicitar información relacionado con su caso, etc.;
- Contactar a los participantes o Titulares para realizar encuestas (encuestas de satisfacción, etc.);
- Contactar a los participantes o Titulares para resolver reclamos, quejas, etc.;

- Remitir a los participantes o Titulares a otros proveedores de servicios para los servicios que necesitan, pero HAI no ofrece;
- Procesar datos para presentar números agregados a nuestros donantes y para informes externos (nunca publicamos datos individuales, solo información agregada, como "Brindamos servicios de asesoramiento para 10,000 personas" etc.);
- Analizar datos para mejorar la calidad del servicio;
- Es posible que, en el caso de una auditoría del donante, nuestros donantes deban revisar nuestros registros, incluidos los datos de los participantes a nivel individual;
- Cumplimiento de la ley colombiana o extranjera y de las órdenes de autoridades judiciales y administrativas;
- Mejora y personalización del contenido que Usted ve en el Sitio, con base en su ubicación geográfica y sus potenciales intereses,
- Ofrecimiento de nuevas atenciones de HAI teniendo en cuenta su ubicación y sus potenciales intereses
- HAI contrata y emplea otras compañías o personas para desarrollar tareas o labores en su nombre o en su beneficio, y con el fin de poder prestar los Servicios, se debe compartir la información del Titular con esas compañías o personas.
- Al suministrarnos su correo electrónico, Usted expresamente nos autoriza a enviarle mensajes por ese medio, y nos autoriza a utilizar el correo electrónico como medio de comunicación con Usted.
- Al suministrarnos su número de teléfono celular, Usted expresamente nos autoriza a enviarle mensajes de texto, de Whatsapp o por cualquier otro sistema digital o tecnológico de mensajería de texto, imagen y/o video por ese medio.
- Los Datos Personales y demás información que Usted nos suministra puede ser utilizada para ser combinada con otra información del Titular o de terceros, obtenida de otras plataformas tecnológicas, sitios o aplicaciones, con el fin de realizar análisis estadísticos y métricas para entender cómo son utilizados los Servicios, y cómo podemos mejorar la experiencia del participante.
- Para validar la información suministrada por Usted;

Los Datos Sensibles que se recolecten, almacenen, administren, custodien, usen o traten de cualquier forma, estarán sujetos al tratamiento y finalidades descritas en precedencia, atendiendo a su naturaleza especial de Datos Sensibles. El Titular no estará obligado a suministrar la información relacionada con Datos Sensibles.

3. Derechos de los Titulares

HAI le informa que Usted, en su calidad de Titular de Datos Personales, tiene los siguientes derechos:

- Conocer, actualizar y corregir sus Datos Personales ante HAI. Este derecho puede ser ejercido, entre otros, en relación con la información parcial, inexacta, incompleta, dividida, información engañosa o cuyo tratamiento sea prohibido o no autorizado.
- Requerir prueba del consentimiento otorgado a HAI para la recolección y el tratamiento de sus Datos Personales, tener acceso a sus Datos Personales que son objeto de tratamiento por parte de HAI y en general, ser informado por HAI del tratamiento que se le está dando a sus Datos Personales.
- Revocar la autorización otorgada a HAI y/o solicitar la supresión de sus Datos Personales cuando Usted considere que HAI no está respetando los principios, derechos y garantías constitucionales y legales.
- Tener acceso a los Datos Personales que HAI haya recolectado y tratado.
- Si Usted no está conforme con la forma en que HAI trata sus Datos Personales o tiene alguna queja o reclamo, podrá presentar un comunicado ante el oficial de protección de datos de HAI al correo electrónico dlozano@heartlandalliance.org
- Si el oficial de protección de datos de HAI no resuelve sus inquietudes o no atiende su queja, Usted podrá dirigirse a la Superintendencia de Industria y Comercio para presentar sus inquietudes, quejas o reclamos si considera que HAI ha violado sus derechos de habeas data o las disposiciones de la Ley 1581 de 2012, el Decreto 1377 de 2013 y otras normas que las modifiquen, adicionen o complementen.

4. Procedimiento y Trámite de Consultas y Reclamos

Las Consultas y/o Reclamos que el Titular desee elevar a HAI se surtirán por medio del siguiente trámite:

4.1. Consultas:

Los Titulares o sus causahabientes podrán consultar la Información Personal elevando solicitud por escrito al correo electrónico contactanos@heartlandalliance.org.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

4.2. Reclamos:

El Titular o sus causahabientes que consideren que la información debe ser objeto de corrección, actualización o supresión, cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en las leyes aplicables, o cuando pretendan revocar la autorización otorgada por medio del presente documento, podrán presentar un reclamo ante HAI, el cual será tramitado bajo las siguientes reglas:

• El reclamo se formulará mediante solicitud escrita dirigida al correo electrónico contactanos@heartlandalliance.org con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

• Una vez recibido el reclamo completo, se incluirá en el sitio donde reposa la información, una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.
• El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.
• El Titular o sus causahabientes sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

5. Tratamiento de Datos Personales de Menores de edad

Los datos personales de los menores de edad tienen una especial protección y por lo tanto su tratamiento está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012 y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.

- Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y su decreto reglamentario.

III. EVALUACIÓN DE RIESGO OPERATIVO & DE SEGURIDAD

El siguiente formato de evaluación de riesgos está adaptado de la matriz de riesgos del Consejo Asesor de Seguridad Exterior. Debe llevarse a cabo una evaluación de riesgo operativo y de seguridad al inicio del programa en un nuevo país. Los evaluadores analizarán la disponibilidad de modos de comunicación, restricciones locales y la probabilidad de interferencia/vigilancia del gobierno. Estos riesgos se evaluarán en función de la gravedad y la probabilidad de riesgos acumulativos. Una vez se determina una calificación de riesgo, los evaluadores determinan si las medidas de mitigación de riesgo pueden reducir efectivamente el nivel de riesgo. Los protocolos de seguridad de la información para lograr este objetivo se enumeran en la siguiente sección.

1. Matriz de evaluación de riesgos

MATRIZ DE EVALUACIÓN DE RIESGOS	**Leyenda:** **U** - Riesgo no gestionable **E** - Riesgo extremo **H** - Alto riesgo **M**- Riesgo medio **L** - Riesgo bajo[20]				
Gravedad (consecuencia o impacto esperado)	**Frecuente**: Sucesos continuos, diarios o inevitables.	**Probable**: Varios o numerosos sucesos. Ocurre semanalmente.	**Ocasional**: Ocurrencias esporádicas o intermitentes. Ocurre mensualmente.	**Raramente**: Ocurrencias poco frecuentes. Ocurre todos los años.	**Improbable**: Posibles sucesos pero improbables
Catastrófico: *Muerte, lesiones graves, pérdida o daño inaceptable de los activos del programa.*	U	E	H	H	M
Crítico: *Alta probabilidad de que la amenaza cause lesiones graves, enfermedad, pérdida o daño de los activos del programa.*	E	H	H	M	L
Moderado: *Podría afectar las operaciones del programa y provocar lesiones, enfermedades, pérdidas o daños leves.*	H	M	M	L	L
Despreciable: *Poco o ningún impacto en las operaciones del programa o en los miembros del personal.*	M	L	L	L	L
Leyenda: **E** - Riesgo extremo **H** - Alto riesgo **M** - Riesgo medio **L** - Riesgo bajo					

[20] Para ver todos los indicadores y una descripción general de los parámetros de evaluación de riesgos, consulte las Instrucciones de evaluación de riesgos, que se pueden encontrar en la unidad O: o adjuntas por separado. Los parámetros y definiciones de puntuación se pueden encontrar en la hoja de instrucciones e indicadores de evaluación de riesgos.

2. -Evaluación de riesgos de seguridad operativa e informática (Por país)

A continuación, encuentra la lista de evaluación específica del riesgo operativo y de seguridad de la información en Colombia.

Los siguientes recursos se utilizaron para evaluar la seguridad operacional y las preocupaciones de seguridad de la información en los países de operación.

- Consejo consultivo de seguridad en el extranjero — Informes criminalísticos y de seguridad
- Restricciones telefónicas SAT — Restricciones telefónicas SAT
- Censura de Facebook Wiki — Censura de FB
- Freedom House — Calificación de libertad de prensa
  Calificación de libertad de la red

COLOMBIA

<table>
<tr><th>INDICADOR DE RIESGO</th><th colspan="2">EVALUACIÓN</th><th>ACLARACIÓN/INFORMACIÓN ADICIONAL</th></tr>
<tr><td rowspan="3">Acceso y confiabilidad de la infraestructura de telecomunicaciones.</td><td>☒ Problemas de latencia de Internet</td><td>☒ Cobertura limitada de telefonía celular</td><td rowspan="3">El acceso a Internet es esporádico y puede verse afectado por las inclemencias del tiempo.
El servicio celular es limitado fuera de las principales ciudades, e inexistente en áreas remotas.
Hay apagones diariamente.</td></tr>
<tr><td>☒ Cortes periódicos de internet</td><td>☒ Cortes telefónicos periódicos</td></tr>
<tr><td>☒ Acceso/disponibilidad limitada de Internet</td><td>☐ Otros</td></tr>
<tr><td rowspan="3">Sitios web restringidos/aplicaciones para teléfonos inteligentes</td><td>☒ Aplicaciones de redes sociales</td><td>☒ Sitios web de redes sociales</td><td rowspan="3">Calificado como "parcialmente gratis" según la calificación de red de Freedom House. El gobierno colombiano intentó enjuiciar a personas en el pasado por compartir artículos críticos en plataformas de redes sociales como Facebook, y ganó una orden judicial para obtener acceso a la cuenta de Facebook de un periodista en julio de 2018. El periodista escribió varios artículos sobre corrupción local para un sitio de noticias.
Se debe suponer que los sitios de redes sociales, las aplicaciones y los sitios web están censurados y pueden estar sujetos a vigilancia.</td></tr>
<tr><td>☒ Aplicaciones de comunicaciones</td><td>☒ Sitios web políticos/religiosos</td></tr>
<tr><td>☒ Sitios web de noticias</td><td>☐ Otros</td></tr>
<tr><td rowspan="3">Restricciones de equipo</td><td>☐ Dispositivos encriptados</td><td>☐ Equipo TSCM</td><td rowspan="3">Los teléfonos satelitales no parecen estar restringidos por el gobierno, pero pueden ser considerados sospechosos o valiosos por los grupos armados. Por lo tanto, los teléfonos satelitales son peligrosos de portar en regiones remotas.</td></tr>
<tr><td>☐ Teléfonos satelitales</td><td>☐ Dispositivos GPS</td></tr>
<tr><td>☐ VPN</td><td>☐ Otros</td></tr>
<tr><td>Cuestiones de vigilancia/contrainteligencia</td><td colspan="3">Las amenazas cibernéticas siguen siendo una preocupación importante de seguridad en Colombia. Los incidentes por motivos políticos han incluido una violación de la cuenta de correo electrónico del presidente Juan Manual Santos y el monitoreo ilegal de las negociaciones de paz de Colombia con las FARC, ambos revelados en febrero de 2014. (OSAC Crimen y seguridad)</td></tr>
<tr><td>Cuestiones de privacidad e integridad de los datos</td><td colspan="3">Las autoridades también informan un número cada vez mayor de ataques motivados financieramente a medida que Colombia amplía el acceso a Internet y los colombianos dependen cada vez más de Internet. El total de quejas por delitos cibernéticos ha aumentado anualmente en cada uno de los años anteriores. Según un estudio de seguridad de Intel, el 15% de los delitos contra empresas en Colombia están asociados con el cibercrimen, generando pérdidas de aproximadamente 600 millones de dólares. (OSAC Crimen y seguridad)</td></tr>
<tr><th colspan="4">CALIFICACIÓN DE RIESGO</th></tr>
<tr><td></td><td>Gravedad</td><td>Frecuencia</td><td>Riesgo</td></tr>
</table>

Leyenda: **U** - Riesgo no gestionable **E** - Riesgo extremo **H** - Alto riesgo **M** - Riesgo medio **L** - Riesgo bajo	Moderado	Ocasional	Medio

Gestión de riesgos

Cinco pasos de la gestión de riesgos: (1) Identificar los peligros (2) Evaluar los peligros (3) Desarrollar controles & tomar decisiones (4) Implementar controles (5) Supervisar y evaluar

PELIGRO	NIVEL DE RIESGO INICIAL	MEDIDA DE MITIGACIÓN/IMPLEMENTADOR	NIVEL DE RIESGO RESIDUAL
Seg. Inf/Op	Medio	No se llevarán teléfonos satelitales. Se adquirirán radios para equipos móviles que viajen a sitios remotos.	Medio

NIVEL DE RIESGO RESIDUAL GENERAL (después de implementar todas las medidas de mitigación)

EXTREMO	ALTO	MEDIO	BAJO
☐	☐	☒	☐

Comité Internacional de la Cruz Roja (CICR). Manual sobre protección de datos en acción humanitaria, 2017. https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

Grupo de trabajo de protección de InterAction. Recolección de datos en respuesta humanitaria: Una guía para incorporar la Protección, 2003. http://www.globalprotectioncluster.org/_assets/files/tools_and_guidance/InterAction_Guide_Incorporating_Protection_2003_EN.pdf

Sphere Association. The Sphere Handbook: Carta humanitaria y normas mínimas en respuesta humanitaria, cuarta edición, Ginebra, Suiza, 2018. www.spherestandards.org/handbook

Comité Permanente entre Organismos. Pautas de gestión de casos de violencia de género, 2017.
Directriz GBVIMS (gestión de casos): Principio rector de UNICEF "Principio 2: derecho a la confidencialidad"
Directriz GBVIMS (gestión de casos): Compromiso inicial con los participantes, explicando la confidencialidad
Directriz GBVIMS (gestión de casos): protocolo de intercambio de información (ISP)

APÉNDICES

APÉNDICE A: Formulario de Reconocimiento de Confidencialidad y Seguridad

HEARTLAND ALLIANCE INTERNATIONAL

FORMULARIO DE RECONOCIMIENTO DE CONFIDENCIALIDAD Y SEGURIDAD

Este reconocimiento aplica a todos los miembros de la fuerza laboral vinculados a tiempo completo o parcial, así como a los miembros de la fuerza laboral no vinculados, incluidos, entre otros, voluntarios, fuerza de trabajo temporal, pasantes, etc.

Heartland Alliance International (HAI) se compromete a proteger la seguridad de nuestra Información Confidencial garantizando que su fuerza laboral y sus afiliados, incluidos consultores, organizaciones asociadas, voluntarios o pasantes, reciban capacitación adecuada y periódica sobre la importancia de la privacidad y la seguridad de la información. El programa de HAI abarca el derecho a la privacidad del participante como parte integral del proceso de asistencia y fundamental para proporcionar el más alto nivel de servicio. Los participantes que creen que su información permanecerá protegida, tienen más probabilidades de proporcionar información completa y precisa, lo que a su vez conduce a un mejor servicio. El uso de cualquier información de los participantes para uso personal o cualquier otro propósito que no sea la operación y el servicio de HAI, está estrictamente prohibido.

HAI tiene la responsabilidad legal y ética de proteger la privacidad y la seguridad de toda la Información Confidencial. Durante su afiliación con HAI, puede escuchar, leer o ponerse en contacto con información relacionada con un participante o ver archivos electrónicos o en papel que pueden contener datos personales.[21], información personal confidencial (ICP)[22]o información privilegiada. También puede crear documentos que contengan dicha información (incluyendo tomar notas, grabar voz, tomar fotos o videos, hacer fotocopias). Esta información se denomina colectivamente "Información Confidencial" y no debe compartirse con otras personas que no tienen una razón legítima para conocer la información.

Como parte de su afiliación con HAI, usted acepta adherirse a lo siguiente con respecto a la confidencialidad y seguridad de la Información Confidencial (lea cuidadosamente y marque todas las casillas):

☐ He leído, entiendo y acepto cumplir con la política de No divulgación de Información Confidencial de HAI y el Deber de discreción y conducta del personal. No accederé, solicitaré ni divulgaré información confidencial sobre la cual no tengo autoridad o que no sea pertinente para mi función.

☐ *Regla básica en el manejo de Información Confidencial.* Solo usaré y divulgaré Información Confidencial según lo permitido o requerido por la ley local aplicable, las políticas de HAI o con la autorización por escrito de los participantes.

☐ *Información Confidencial.* Consideraré toda confidencialidad como una obligación central de mi afiliación con HAI. Salvo lo permitido por este Reconocimiento, en ningún momento, durante o después

[21] Los datos personales se refieren a la información que se puede utilizar para distinguir o rastrear la identidad de un individuo, ya sea independientemente o cuando se combina con otra información personal o de identificación. Para obtener una definición detallada, consulte el Glosario de Términos en el manual de HAI.

[22] La información confidencial personal (ICP) se refiere a la información que es privada o podría dañar a un individuo si se hace pública. Los ejemplos incluyen: origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, y el procesamiento de datos genéticos, datos biométricos, datos sobre la salud (por ejemplo, salud mental o estado de VIH), datos sobre la vida u orientación sexual de una persona natural.

de mi afiliación con HAI, hablaré, compartiré o permitiré que ninguna persona no autorizada examine ningún archivo electrónico o físico que contenga Información Confidencial.

☐ *Uso y divulgación permitidos (no se necesita autorización).* Entiendo que puedo usar y divulgar Información Confidencial **solamente** cuando el propósito de la divulgación se incluya dentro de lo siguiente:

- La Información Confidencial se usa o divulga al participante que es el sujeto de dicha información.
- El uso o divulgación de Información Confidencial es necesario para la seguridad física y mental de los participantes, incluida la denuncia de acoso sexual, explotación y abuso.
- El uso o divulgación de Información Confidencial es necesario para el tratamiento médico, pago u operación de atención médica.
- El uso o divulgación de Información Confidencial es obligatorio bajo las leyes de informes obligatorios en el país de operación.

☐ *Proceso de aprobación.* Entiendo que primero debo buscar una aprobación de la administración de HAI para fines comerciales fuera de los casos enumerados en *excepciones a la no divulgación de Información Confidencial*. Debo esperar la aprobación de la administración de HAI para obtener el formulario de autorización apropiado firmado por los participantes que dan su consentimiento. Entiendo que no se me permite participar en ninguna actividad, como registrar o divulgar información de los participantes hasta que obtenga la aprobación de la administración de HAI.

☐ *Deber de informar.* Acepto informar de inmediato a mi supervisor y/o al Director de País de HAI y/o al Director de Riesgos de HA cualquier divulgación no permitida de Información Confidencial que realice por accidente o por error. También informaré sobre cualquier uso o divulgación de Información Confidencial que vea o conozca de otros que pueda constituir una divulgación ilícita.

☐ *Salvaguardas* Durante el transcurso de mi afiliación con HAI, si debo analizar la Información Confidencial con otros miembros de la Fuerza laboral de HAI para realizar mis funciones designadas, aplicaré discreción para asegurarme de que terceros y/o empleados no autorizados no puedan escuchar esas conversaciones. Entiendo que cuando la Información Confidencial está bajo mi control, debo usar todos los medios razonables para protegerla.

☐ *Seguridad de dispositivos electrónicos.* Acepto no descargar Información Confidencial en dispositivos electrónicos de propiedad personal. Nunca intentaré acceder a la información utilizando un código de identificación de usuario o contraseña que no sea el mío, ni divulgaré mi código de identificación de usuario o contraseña a nadie, ni permitiré que ninguna persona acceda o altere Información Confidencial bajo mi identidad.

☐ *Uso de internet*. Estoy de acuerdo en nunca almacenar, compartir o transmitir Información Confidencial en sitios de Internet (por ejemplo, sitios web, blogs, publicaciones en redes sociales, etc.) que no hayan sido aprobados por HAI para ingresar al dominio público. Estoy de acuerdo en nunca comunicarme con los participantes a través de sitios de redes sociales y nunca publicar comentarios como si estuviera actuando en nombre de HAI a menos que se me haya dado específicamente permiso previo para hacerlo.

☐ *Seguridad física.* Tomaré todas las precauciones razonables, bajo mi control, para salvaguardar la Información Confidencial. Esto incluye tomar los pasos necesarios para asegurar que mi computadora esté bloqueada cuando estoy lejos de mi estación de trabajo y asegurar apropiadamente la propiedad de la compañía en mi posesión.

☐ *Devolución o destrucción de información.* Si mi afiliación con HAI requiere que saque la Información Confidencial de la oficina de HAI o la propiedad de los afiliados de HAI, me aseguraré de tener el permiso apropiado para hacerlo. Protegeré la Información Confidencial de la divulgación no autorizada a otros, y me aseguraré de que toda la Información Confidencial se devuelva al centro de HAI correspondiente.

Entiendo que, en caso de que la Información Confidencial deba ser destruida, mi supervisor me instruirá sobre el tipo de información a ser destruida y el método apropiado de destrucción. No destruiré información original a menos que mi supervisor me haya indicado que lo haga.

☐ *Terminación.* Una vez finalice mi afiliación con HAI, me aseguraré de no llevarme Información Confidencial y devolveré toda la Información Confidencial que posea a HAI. Si no se trata de documentos originales, sino más bien de mis propias notas personales desarrolladas durante el transcurso de mi afiliación con HAI, debo entregar esa información a HAI. El despido o desvinculación, ya sea voluntaria o no, no afectará mi obligación continua de salvaguardar la confidencialidad y seguridad de la Información Confidencial.

Entiendo que ninguna parte de este Reconocimiento me impide hacer una divulgación de Información Confidencial si la ley me exige que lo haga.

Mi firma a continuación reconoce que he leído los términos y condiciones de este Reconocimiento. El supervisor de área mantendrá la página de firmas.

Con mi firma a continuación, reconozco que he leído los términos y condiciones del Reconocimiento de confidencialidad/seguridad. Entiendo que las violaciones de este Reconocimiento pueden resultar en el rechazo de mi afiliación con Heartland Alliance International. Además, entiendo que este reconocimiento no restringe ni prohíbe, de ninguna manera, mi capacidad y obligación de denunciar sospechas de fraude, derroche o abuso.

Certifico con mi firma a continuación que he leído que acataré la política y los protocolos relacionados con la confidencialidad.

NOMBRE IMPRESO

FIRMA

FECHA

TÍTULO DEL CARGO

ORGANIZACIÓN/AFILIACIÓN

LAS PREGUNTAS, CONSULTAS O REPORTES DE VIOLACIONES PUEDEN SER DIRIGIDAS A:

NOMBRE	Jakson Phillips Delgado
CARGO	Security Officer
TELÉFONO	+57(2) 3899752
DIRECCIÓN DE CORREO ELECTRÓNICO	<jphillips@heartlandalliance.org>

APÉNDICE B: INSTRUCCIONES PARA RECUPERAR CORREOS ELECTRÓNICOS ENVIADOS A PERSONAS EQUIVOCADAS

El envío accidental de un correo electrónico con Información Confidencial a la persona equivocada constituye un incidente de violación. A continuación, se encuentran las instrucciones para recuperar un correo electrónico enviado accidentalmente a la persona equivocada. Esto solo funciona en Microsoft Outlook. Se desaconseja enviar y recibir Información Confidencial por correo electrónico porque es muy vulnerable a errores humanos como este.

Paso 1: Vaya a la carpeta 'Enviados'.

Paso 2: Haga doble clic en el correo electrónico que desea recuperar para que se abra en una nueva ventana.

Paso 3: En el menú desplegable Acciones, seleccione "recuperar mensaje".

Paso 4: Elija si desea eliminar copias no leídas o eliminar y reemplazar con un nuevo mensaje. Haga clic en "Aceptar" cuando haya terminado. Cuando se elimine correctamente, recibirá un correo electrónico confirmando la eliminación.

Paso 5: Guarde el correo electrónico de confirmación e inclúyalo en el informe de RMIS o proporciónelo al investigador del posible incidente de incumplimiento.

APÉNDICE C: Guía paso a paso para compartir de forma segura

1. Archivos electrónicos compartidos USANDO CORREO ELECTRÓNICO

- Marque el archivo electrónico como confidencial.

  Los archivos electrónicos que contienen Información Confidencial deben tener marcas explícitas que indiquen su naturaleza confidencial. Use cualquiera de los siguientes métodos:

  a) Coloque una marca de agua de identificación "CONFIDENCIAL".

     : En Microsoft Word, seleccione la pestaña "Diseño" - haga clic en "Marca de agua" en el lado derecho de la página - haga clic en "CONFIDENCIAL"

  b) Inserte texto en el encabezado o pie de página del documento señalando que es "confidencial", "no para su distribución" u otra marca que lo designe como confidencial.

Propósito	Autorización del supervisor/director de país	Consentimiento informado de los participantes.	Ejemplos:
Función central del trabajo	No	Sí, durante la admisión (si la información involucra información identificable individualmente) No, si no es información relacionada con el participante	Abogados que toman notas para brindar asesoría legal, trabajadores capacitados que toman notas de la sesión de SSMAP; trabajadores sociales que diligencian formularios de admisión y toman notas de gestión de casos; persona que ingresa datos que inserta datos de participantes en el rastreador de casos/base de datos; gerente de seguridad que recopila y documenta información relacionada con la seguridad de la operación de HAI;
Periférico a la función de trabajo de la persona	Sí	Sí, si la información involucra información identificable individualmente No, si no hay información identificable individualmente	