Continuidad de la atención médica (CoC) de la ciudad de Watsonville, condado de Santa Cruz
Póliza de seguridad del sistema de información para la gestión de personas sin hogar (HMIS)

Esta Póliza describe los estándares de seguridad de la información de identificación personal recopilada y almacenada en el HMIS de CoC de la ciudad de Watsonville, condado de Santa Cruz. Los estándares pretenden garantizar la seguridad de la información personal. Esta Póliza de seguridad ("Políza") se basa en los principios de prácticas de información justas reconocidas por las comunidades de seguridad y tecnología de la información y las pautas del HMIS del Departamento de Desarrollo Urbano y Vivienda (HUD): (https://www.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf).

Esta Póliza define los estándares de seguridad que deben cumplir las organizaciones dentro del sistema de CoC que registran, usan o procesan información de identificación personal (IIP) de los consumidores en riesgo de sufrir o que están sufriendo la falta de vivienda para el HMIS. Las organizaciones también deben cumplir con las leyes federales, estatales y locales que exigen medidas adicionales para la protección de la seguridad, cuando corresponda.

Esta Póliza reconoce la amplia diversidad de organizaciones que participan en el HMIS, así como las diferentes realidades programáticas y organizativas que podrían exigir un estándar más alto para algunas actividades. Algunas organizaciones, por ejemplo, aquellas que atienden a víctimas de violencia doméstica, podrían optar por implementar estándares más altos de seguridad dada la naturaleza de los consumidores atendidos o de los servicios específicos ofrecidos. Otras, por ejemplo, los refugios de emergencia más grandes, podrían determinar que los estándares más altos son demasiado complicados o inviables. Sin embargo, todas las organizaciones deben cumplir, como mínimo, con los estándares de seguridad descritos en esta políza. Este enfoque ofrece un *estándar mínimo* uniforme de privacidad y protección de la seguridad de los datos para los consumidores que corren el riesgo de sufrir o sufren la falta de vivienda, con la posibilidad de agregar protecciones más restrictivas en el caso de organizaciones que tienen necesidades o capacidades adicionales.

En las siguientes secciones se analizan los estándares de seguridad del HMIS.

I. Estándares de seguridad del HMIS: Definiciones

A. *Información de identificación personal (IIP):* Toda información que una organización para personas sin hogar cubierta mantiene sobre un consumidor en riesgo de sufrir o que sufre la falta de vivienda que: (1) identifique, ya sea directa o indirectamente, a una persona individual; (2) pueda manipularse con un método razonablemente previsible con el fin de identificar a una persona individual; o (3) pueda asociarse con otra información disponible con el fin de identificar a una persona individual.

B. *Organización para personas sin hogar cubierta (CHO):* Toda organización,

incluidos sus empleados, voluntarios, afiliados, contratistas y asociados, que registra, usa o procesa IIP de los consumidores en riesgo de sufrir o que están sufriendo la falta de vivienda para el HMIS de CoC de Watsonville/Santa Cruz. Esta definición incluye tanto a las organizaciones que tienen acceso directo al HMIS como a las que no lo tienen, pero que registran, usan o procesan IIP del HMIS.

C. *Procesamiento:* Toda operación o conjunto de operaciones realizadas respecto de la IIP, ya sea con medios automáticos o no, incluidos la recopilación, el mantenimiento, el uso, la divulgación, la transmisión y la destrucción de la información, entre otros.

II. Estándares de seguridad

En esta sección se describen los estándares de seguridad de sistemas, aplicaciones y copias impresas. Todas las CHO deben cumplir con estos requisitos.

Seguridad de sistemas

A. *Seguridad de equipos* Una CHO debe proporcionar disposiciones de seguridad en todos los sistemas en los que se almacene IIP, incluidas redes, computadoras de escritorio, computadoras portátiles, minicomputadoras, servidores y procesadores centrales de la CHO, entre otros. Una CHO debe proporcionar disposiciones de seguridad en todos los sistemas en los que se almacene IIP, incluidas redes, computadoras de escritorio, computadoras portátiles, minicomputadoras, tabletas, teléfonos celulares, servidores y procesadores centrales, entre otros.

Las CHO que usen dispositivos móviles deben estipular medidas de seguridad adicionales de los equipos para el uso de dispositivos en el campo. Los usuarios del HMIS solo deben usar dispositivos empresariales en lugar de personales para acceder al HMIS. Los dispositivos móviles deben estar cifrados. Esta funcionalidad está integrada en las últimas versiones de Android e iOS. Se debe acceder al HMIS a través de una ventana privada del navegador, por ejemplo, una ventana de incógnito en Chrome, o cambiando la configuración del navegador para que no guarde los datos de formularios (es decir, llenado automático) o el guardado en caché de la página (esto no es posible en todas las páginas). Los dispositivos deben permitir la gestión de perfil o dispositivo remota de los administradores de TI de CHO. Tanto iOS como Android tienen una funcionalidad que permite ubicar y, si es necesario, borrar los dispositivos perdidos o afectados. Los dispositivos móviles deben usar una conexión celular integrada o un punto de acceso wifi celular con una conexión cifrada. Los puntos de acceso wifi públicos NO se pueden usar para conectarse al HMIS. Se debe usar una conexión VPN para mejorar la seguridad de la conexión siempre que sea posible.

B. *Autenticación del usuario:* Cada usuario que acceda a una máquina que tenga datos del HMIS debe tener un nombre de usuario y una contraseña únicos. Las contraseñas deben tener al menos ocho caracteres y cumplir con los requisitos estándares razonables de la industria. Estos requisitos deben incluir, entre otros, lo siguiente:

1. Usar al menos un número y una letra o símbolo
2. No usar ni incluir el nombre de usuario, el nombre de HMIS o el nombre del proveedor de HMIS
3. No tener únicamente una palabra que esté en el diccionario común ni

palabras deletreadas en orden inverso

Información escrita que corresponde específicamente al acceso del usuario, por ejemplo, el nombre de usuario y la contraseña no deben almacenarse ni mostrarse en un lugar de acceso público. Los usuarios individuales no deben registrarse en más de una estación de trabajo al mismo tiempo ni deben registrarse en la red en más de una ubicación al mismo tiempo.

C. *Protección contra virus:* Una CHO debe proteger el HMIS y los dispositivos electrónicos usados para almacenar IIP contra virus mediante el uso de software de protección contra virus comerciales. La protección contra virus debe incluir el escaneo automático de archivos cuando los usuarios acceden a ellos en el sistema en el que está la aplicación de HMIS. Una CHO debe actualizar periódicamente las definiciones de virus del proveedor de software.

D. *Firewalls:* Una CHO debe proteger el HMIS y los dispositivos electrónicos usados para almacenar IIP contra intrusión maliciosa con un firewall seguro. Cada estación de trabajo individual no necesita contar con su propio firewall, siempre que haya un firewall entre la estación y los sistemas, incluido internet y otras redes informáticas, ubicados fuera de la organización.

Por ejemplo, una estación de trabajo que accede a internet a través de un módem necesitaría su propio firewall. Una estación de trabajo que accede a internet a través de un servidor central no necesitaría un firewall si el servidor ya cuenta con uno. Los firewalls se incluyen comúnmente en los sistemas operativos nuevos. Los sistemas operativos más antiguos pueden equiparse con firewalls seguros que se pueden comprar o conseguir gratis en internet.

E. *Acceso público:* El HMIS y cualquier dispositivo electrónico usados para almacenar IIP que usen foros públicos para la recolección y la información de datos deben estar protegidos para permitir únicamente conexiones de computadoras y sistemas aprobados a través de certificados de infraestructura de claves públicas (PKI) o extranets que limiten el acceso basado en la dirección del proveedor de internet (IP), o medios similares. Un foro público incluye sistemas con acceso público a cualquier parte de la computadora a través de internet, módems, tableros de anuncios, quioscos públicos o campos similares.

F. *Acceso físico a sistemas con acceso a los datos del HMIS:* Una CHO siempre debe contar con computadoras en áreas públicas que se usen para recopilar y almacenar datos del HMIS. Cuando las estaciones de trabajo no estén en uso y el personal no esté presente, se deben tomar medidas para garantizar que las computadoras y los datos estén protegidos y no puedan usarlos personas no autorizadas. Las estaciones de trabajo que no estén en uso temporalmente deben activar automáticamente un salvapantallas protegido con contraseña. Los salvapantallas protegidos con contraseña son una función estándar de la mayoría de los sistemas operativos, y la cantidad de tiempo puede regularla la CHO. Si el personal de una CHO se ausenta durante un período prolongado, debe cerrar sesión en el sistema de ingreso de datos y apagar la computadora.

G. *Protección y recuperación ante desastres:* Los datos del HMIS deben copiarse periódicamente en otro medio y almacenarse en un lugar seguro fuera del sitio que cuente con los estándares de seguridad. Una CHO que almacene datos (Bitfocus) en un servidor central debe contar con servidores en una habitación segura que

tenga los sistemas adecuados de control de temperatura y extinción de incendios. Los supresores de sobrecarga se usan para proteger los sistemas usados para recopilar y almacenar todos los datos del HMIS.

H. ***Eliminación:*** Para borrar todos los datos del HMIS de un medio de almacenamiento, una CHO debe reformatear el medio de almacenamiento. Una CHO debe reformatear el medio de almacenamiento más de una vez antes de reutilizar o eliminar el medio.

I. ***Supervisión de sistemas:*** Una CHO debe usar métodos adecuados para supervisar los sistemas de seguridad. Los sistemas que tienen acceso a los datos del HMIS deben mantener un registro del acceso de los usuarios. Muchos sistemas operativos y servidores web nuevos están equipados con registros de acceso, y algunos permiten a la computadora enviar por correo electrónico la información de registro a un usuario designado, generalmente, el administrador del sistema. Los registros deben verificarse de forma rutinaria.

Seguridad de aplicaciones

A. ***Aplicabilidad:*** Una CHO debe aplicar disposiciones de seguridad para aplicaciones al software durante el ingreso, el almacenamiento y la revisión de datos u otra función de procesamiento.

B. ***Transmisión electrónica de datos:*** Una CHO debe cifrar todos los datos del HMIS que se transmitan de forma electrónica por internet, redes de acceso público o líneas telefónicas según los estándares industriales actuales. El estándar actual es el cifrado de 128 bits. Los datos no cifrados deben transmitirse por conexiones directas seguras entre dos sistemas. Una conexión directa segura es aquella a la que solo pueden acceder usuarios que han sido autenticados al menos en uno de los sistemas involucrados y que no usan sistemas terciarios para transmitir los datos. Una red segura tendría conexiones directas seguras.

C. ***Almacenamiento electrónico de datos:*** Una CHO debe almacenar todos los datos del HMIS en formato binario, no de texto. Una CHO que usa una de las diversas aplicaciones comunes, por ejemplo, Microsoft Access, Microsoft SQL Server u Oracle, ya almacena los datos en formato binario y no debe tomar otras medidas.

Seguridad de copias impresas

A. ***Aplicabilidad:*** Una CHO debe proteger todo documento o copia impresa que tenga IIP generada por el HMIS o para este, pero que no se limita a informes, formularios de ingreso de datos y notas de casos/consumidores. Las copias impresas deben almacenarse en un archivador seguro cerrado en un área que no sea accesible para personal que no pertenezca a la CHO.

B. ***Seguridad:*** Una CHO siempre debe supervisar todo documento o copia impresa generada por el HMIS o para este que tenga IIP cuando la copia impresa está en un lugar público. Cuando el personal de la CHO no está presente, la información debe guardarse en lugares que no sean de acceso público. Información escrita que corresponde específicamente al acceso del usuario, por ejemplo, el nombre de usuario y la contraseña no deben almacenarse ni mostrarse en un lugar de acceso público.