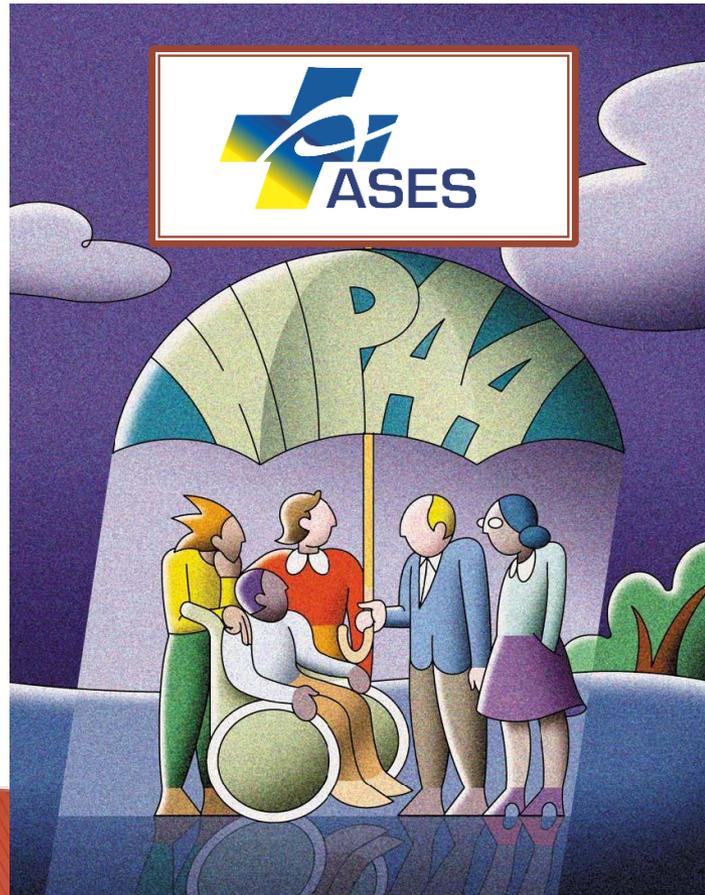


# Políticas y Procedimientos de Privacidad- Ley HIPAA



# Ley HIPAA–Ley de Portabilidad y Responsabilidad de Seguros de Salud 104–191–1996

## Objetivo Primordial

### Privacidad

- El implementar las medidas y controles que regulen la distribución y acceso a la Información médica de pacientes. (Hablada, escrita o electrónicamente, entre otros medios.)

### Seguridad

- Imponer medidas de seguridad que garanticen el cumplimiento con la privacidad de la información del paciente.

## ▶ Información de Salud Protegida:

❑ Cualquier información de salud que identifica a una persona y que es utilizada o divulgada por una agencia cubierta (Aseguradoras, Proveedores de Servicio Médico “*clearing houses*”, Agencias Reguladoras por el Departamento de Salud Federal)

❑ Se incluye en ella:

- Condiciones del presente, pasado, y futuro
- Cualquier provisión de cuidado médico
- Pagos pasados, presentes o futuros relacionados al cuidado médico

# Política de Privacidad 2.1 Acceso por Personal de ASES -SISTEMA HCRE

Director Ejecutivo y Sub-Director Ejecutivo

El personal de ASES autorizado a tener acceso a la información de salud del Beneficiario de Mi Salud en el Sistema HCRE:

Director y Supervisor de Servicio al Cliente

Representantes de Servicio al Cliente y Asistente Administrativo

Director y Director Auxiliar de Asuntos Fiscales

Director de Planificación

Analista de Contabilidad I y II

Director y Director Auxiliar de Sistemas de Información

Todo empleado que necesite acceso a la información del beneficiario, debe ser solicitado por el Director de su área de acuerdo a los procedimientos establecidos por ASES y establecer justificaciones para el acceso del empleado.

## 2.1 – Solicitud de Acceso a la Información de Salud del Beneficiario

- ▶ Por parte de Beneficiario
  - Debe ser solicitado al Oficial de Privacidad
  - Debe ser por escrito
  - Utilizar Hoja de Solicitud de Acceso
  
- ▶ Excepciones:
  
- ▶ Todo beneficiario tiene derecho al acceso de información de salud excepto en:
  - Notas de psicoterapia
  - Información compilada para procesos Judiciales, Administrativos y Criminales
  - Información obtenida de fuentes confidenciales si al obtener la información se revelará la fuente confidencial.

## 2.1. – Conjunto de Record Designado

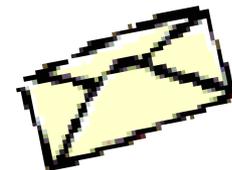
- ▶ Todos los records mantenidos por ASES son parte del Conjunto de Records Designados:
  - Suscripción
  - Pago
  - Adjudicación de Querellas o Reclamaciones
  - Administración de casos o sistemas de records médicos.
  - Cualquier record utilizado por ASES para realizar cualquier determinación sobre el beneficiario.

## 2.2–Solicitud de Contabilidad de Información de Salud

- ▶ El Oficial de Privacidad deberá mantener un Registro de las Autorizaciones provistas por el beneficiario para utilizar o divulgar su información de salud protegida, así como la documentación generada para atender las solicitudes emitidas en situaciones de emergencias y querellas o reclamaciones radicada por un beneficiario, por un periodo de seis (6) años desde la fecha que se solicitó la información. Esto incluye pero no se limita a comunicaciones realizadas por fax, correspondencia y teléfono.
  
- ▶ Registro incluirá:
  - Fecha de divulgación de la información
  - Nombre de la entidad o persona que recibió la información
  - Dirección de la persona que recibió información de salud del beneficiario, de conocerse.
  - Breve descripción de la información de salud protegida divulgada
  - Breve declaración del propósito de la divulgación

## 3.1.5–Solicitud de Comunicaciones Alternas

- ▶ ASES permitirá que los Beneficiarios soliciten que se utilice métodos alternos de comunicación u otros medios al enviar comunicación que contenga información de salud protegida según establecido en las normas de privacidad de HIPPA, en caso que la divulgación de dicha información, toda o parte de ella, podría poner en riesgo la vida del beneficiario.
- ▶ El Representante de Servicio al Cliente debe utilizar su juicio profesional en situaciones que indiquen riesgo a la salud o vida del beneficiario y realizar los arreglos necesarios para enviar la comunicaciones a una dirección alterna, de ser necesario, si no pueden acceder a la dirección oficial del solicitante.



## 2.4 Utilización y Divulgación General de Información de Salud Protegida

- ▶ ASES puede utilizar y divulgar información de salud protegida para fines de tratamiento, pago, y operaciones de salud sin necesitar la autorización expresa de beneficiario o la oportunidad al beneficiario de objetar la divulgación.
- ▶ Si no es para estos fines ASES necesitará la autorización expresa autorizada por el Beneficiario para poder divulgar cualquier información de salud y cumplir con el requisito de mínimo necesario.
- ▶ En caso de que sea necesario, a juicio del Representante de ASES, se le denegará la información de salud Protegida aunque esté autorizada por el beneficiario. Esto sucede si dicha autorización ha caducado o si el Representante de ASES puede pensar que la entidad a quien se le proveerá la información no cumple con los requisitos de confiabilidad establecidos por Ley.

## 3.11 –Divulgación de Información de Salud por Teléfono



- ▶ Toda llamada recibida en el Área de Servicio al Cliente debe ser registrada según los procedimientos establecidos para estos propósitos.
- ▶ El representante de servicio debe ejercer su juicio profesional para divulgar la información de salud protegida estrictamente necesaria para cumplir con la solicitud.
- ▶ Si el representante no está seguro que la persona que estableció la comunicación es el beneficiario o su representante autorizado, debe consultar con su supervisor o el Oficial de Privacidad antes de divulgar cualquier información.
- ▶ Si lo que solicita, el beneficiario tiene que ver con información psiquiátrica, relacionada al abuso y/o tratamiento de drogas o alcohol, relacionada a violencia doméstica y/o diagnósticos o tratamiento de VIH, no debe ser comunicada vía telefónica.

# Divulgación de Información de Salud Protegida por Correo Electrónico



- ▶ Esta política establece salvaguardar procedimientos a seguir por los empleados de ASES al intercambiar información de salud protegida de los beneficiarios por correo electrónico.
- ▶ Representante de ASES deberá verificar la dirección de correo electrónico del recipiente de la información antes de enviar el correo electrónico si este es conocido por ASES.
- ▶ De no ser conocido, el representante de ASES debe seguir primero los procesos para verificar la identidad y autoridad de la persona que recibirá la información.
- ▶ La información enviada debe contener solamente el mínimo de información necesaria para los propósitos que es requerida y debe incluir solamente la información que se relacione directamente con la necesidad de información del recipiente.

- ▶ La utilización de correo electrónico para divulgar información de salud de un beneficiario referente a VIH, abuso de sustancias controladas, abuso de alcohol o información psiquiátrica o de salud mental, **solamente es permitida en circunstancias extraordinarias con la aprobación del Oficial de Privacidad.**

Solamente procederá cuando entregando la información a mano o por correo certificado no cumpliría con la necesidad urgente del cuidado o tratamiento del beneficiario. Para propósitos administrativos, deben ser omitidos el nombre del beneficiario y otros elementos que puedan identificarlo, para propósitos clínicos, el correo debe contener solamente el identificador del beneficiario y su fecha de nacimiento.

- ▶ Si el empleado de ASES se percata de un correo electrónico que contiene información de salud protegida, se envió a una persona para la cual no estaba dirigida la información, deberá reportar dicho incidente inmediatamente al Oficial de Privacidad y proveerle al detalle las circunstancias de la divulgación.
- ▶ En estos casos el Oficial de Privacidad deberá registrar en la base de datos de divulgaciones y evaluar la medida para mitigar el efecto del incidente de la divulgación.

- ▶ Los correos electrónicos referentes a los beneficiarios deben ser enviados solamente a través de los sistemas de información y la Red de ASES.
- ▶ Los empleados de ASES no pueden utilizar sus cuentas personales de correo electrónico para transmitir información de salud protegida a un beneficiario.
- ▶ Al momento de enviar un correo electrónico que contenga información de salud protegida a varios recipientes. **NO** Utilizar grupos de correspondencia pre definidos, ya que los recipientes de la información pueden variar sin percatarse.
- ▶ Si al divulgar la información se realiza para propósitos que no es requerido una autorización, el Representante de ASES debe registrar la divulgación en la base de datos de divulgaciones.
- ▶ Si el empleado que envía el correo electrónico no tiene acceso a la base de datos del Registro de Divulgaciones, el empleado deberá notificar al Oficial de Privacidad de la divulgación realizada y este deberá ser quien la registre.

- ▶ ASES en este momento no cuenta con un Programa para encriptar los correos electrónicos que salen al exterior. Nos encontramos en ese proceso.
  
- ▶ De surgir la necesidad que la Información de Salud Protegida Electrónica se puede realizar la siguiente manera.
  - Grabar documento antes de enviarlo
  
  - En el área de guardarlo existe una alternativa llamada “tools”, que se encuentra al lado de la tecla “save”
  
  - En la tecla “tools” se busca la opción “general option” y en esta opción “read only”.
  
  - Luego de enviar este correo se le enviará al recipiente otro correo indicando la contraseña que utilizará para abrir el correo.



# Divulgación por Fax de Información de Salud

- ▶ El envío de información de salud protegida para propósitos de pago, tratamiento u operaciones de cuidado de salud es permitido, siempre y cuando se sigan los requisitos descritos en las políticas y procedimientos de privacidad de ASES para estos fines.
- ▶ Si es para propósitos que no sean de pagos, tratamiento u operaciones de salud, se puede hacer siempre y cuando se obtenga autorización del beneficiario, según lo requerido por HIPAA.
- ▶ Todo tipo de comunicación enviada a través de Fax que contenga información de salud protegida de un beneficiario debe contener una notificación o advertencia de confidencialidad.
- ▶ La información enviada debe contener la información mínima necesaria para los propósitos que se necesita.

- ▶ A menos que sea estrictamente necesario, los nombres de los pacientes deben ser removidos antes de enviar el fax.
- ▶ El Fax debe tener un “*cover sheet*” y el mismo será guardado junto con la información y con la confirmación del envío.
- ▶ El que recibe el Fax debe ser previamente notificado para indicar la que la información enviada solamente contiene el número de identificación del paciente. Luego de ser enviado, hay que llamar al recipiente para verificar que la información fue recibida.
- ▶ Anotar en la hoja de confirmación la fecha y hora de envío y nombre de la persona con la que se habló. Este documento, junto con la información enviada deberá ser guardado en un lugar seguro.
- ▶ Los números que frecuentemente se marcan para enviar ésta información vía fax, deben ser programados en la máquina de Fax para eliminar errores en la transmisión o errores al marcar un número.
- ▶ Es responsabilidad de los Directores verificar que los números pre-programados en la máquina de Fax son los correctos o estén actualizados. Esta revisión se debe realizar por lo menos anualmente.

# Uso, Divulgación y solicitud de Mínimo Necesario

- ▶ El requisito de la Información Mínima necesaria establece que la información a ser divulgada será la información necesaria para resolver cualquier asunto o situación presentada, por lo que ASES no debe proveer más información de la necesaria.
- ▶ ASES no puede divulgar información de Salud Protegida a otra entidad no cubierta por HIPAA sin la Autorización expresa del beneficiario. Esta solicitud debe ser consistente con la autorización escrita por el beneficiario y cumplir con el requisito de la Información Mínima Necesaria en todo momento.

## 3.6–Notificación de Prácticas de Privacidad

- ▶ Es responsabilidad de ASES proveer una notificación de sus prácticas de privacidad a los beneficiarios de Mi Salud en la cual se debe describir el uso y la divulgación de la información de salud protegida para los beneficiarios y donde se indiquen sus derechos y las responsabilidades de ASES para con ellos.
- ▶ Esta notificación debe ser entregada al momento que el beneficiario es elegible para participar del Plan del Gobierno del Estado Libre Asociado.

## Política de Privacidad 3.2.1 – Querellas o Reclamaciones de Privacidad

- ▶ Esta política establece que los procedimientos para que los beneficiarios puedan radicar querellas sobre el cumplimiento de ASES con sus políticas y Procedimientos de Privacidad establecidos para el cumplimiento con las normas federales de privacidad.
- ▶ La presentación de cualquier tipo de querella de beneficiarios, proveedores de servicios o aseguradoras relacionadas a la violación de información de salud protegida, debe someterse por escrito.
- ▶ Esta debe contener el acto que alegadamente se violó, la reglamentación de privacidad y fecha de dicha violación.

## Política de Privacidad 3.13– Identificación y Verificación

- ▶ Los empleados de ASES ejercerán su juicio profesional para verificar, antes de divulgar cualquier información de salud de un beneficiario, la identidad y autoridad de los oficiales públicos y los oficiales que no son públicos que soliciten tener algún tipo de acceso a información de salud específica si la identidad del solicitante no es conocida.
- ▶ Esta política es para establecer la suficiente seguridad para evitar divulgaciones inapropiadas o impropias de la información de salud de un beneficiario.

## Política de Privacidad 3.12– Adiestramiento de Empleados

- ▶ Es responsabilidad de ASES proveer a todos los empleados nuevos en posiciones temporeros o regulares o por contrato, un adiestramiento de las políticas y procedimientos de privacidad de ASES en un tiempo razonable.
- ▶ Además, proveer un adiestramiento a los empleados afectados por las modificaciones realizadas a las políticas o procedimientos de privacidad de ASES.
- ▶ El readiestramiento de los empleados deber ser realizado no más tarde de los 30 días del cambio en el procedimiento o política.



# Política de Privacidad 3.10– Seguridad Física

- ▶ **Almacenamiento de documentos:** Al final del día, los documentos de ASES que contengan información de salud protegida de los beneficiarios se deben localizar en archivos seguros y bajo llave.
- ▶ **Impresoras:** Las impresoras no deben estar localizadas en áreas comunes o cerca de los pasillos en los cuales cualquier persona, visitante o empleado tengan acceso. Documentos deben ser recogidos lo antes posibles. Supervisores deben verificar por lo menos una vez al día que se este cumpliendo con esta política.
- ▶ **Máquinas de Fax:** El fax debe estar localizado en un área segura y controlada para que la información que se reciba o se envíe no este accesible. Documentos deben ser recogidos inmediatamente.
- ▶ **Seguridad de Sistema de Información:** Empleados deben utilizar “*Screen Savers*” Identificación de usuarios contraseñas y otras medidas de seguridad para mantener el control en el acceso de información.
- ▶ **Otros:** Las conversaciones con los beneficiarios deben ser privadas y confidenciales.

# Seguridad

- ▶ Ha habido una serie de incidentes de seguridad relacionados con el uso de ordenadores portátiles, otros dispositivos portátiles o móviles, USB y “Hardware” externos que almacenan, contienen o se utilizan para acceder información de Salud Protegida Electrónica.
- ▶ CMS ha delegado autoridad para hacer cumplir las normas de seguridad de HIPAA y verificar si las acciones de una entidad cubierta son razonables y apropiadas para proteger la confidencialidad, Integridad y disponibilidad de una Información de Salud Protegida Electrónica.

► Los tipos de dispositivos y herramientas sobre el cual existe esta preocupación por su vulnerabilidad, incluyen:

- Ordenadores Portátiles
- Computadoras Personales
- Teléfonos Inteligentes y PDAs,
- Hoteles
- Bibliotecas, o
- Estaciones de trabajo publico
- Puntos de acceso inalámbricos
- USB
- Tarjetas de Memorias
- CDs, DVD,
- Medios de Backup

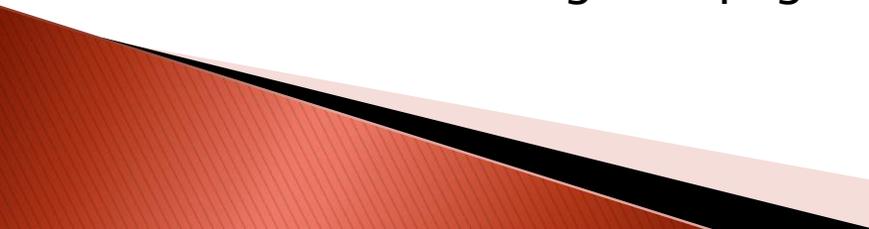
- ▶ En relación con el acceso remoto o uso Información de Salud Protegida Electrónica, las entidades cubiertas deben poner en gran énfasis y atención en su:
    - Análisis de Riesgo y Estrategias de gestión de riesgo
    - Políticas y Procedimientos para proteger la información
    - Sensibilización de Seguridad
- 

# Establecer Política de Sanción

- ▶ Una Política de Sanciones debe estar establecida en el lugar de trabajo y la misma debe ser comunicada efectivamente para que los empleados entiendan las consecuencias de no cumplir con las políticas de seguridad y procedimientos en la entidad cubierta.
  - ▶ Esta debe ser un requerimiento para que los empleados la comprendan y firmen una declaración de adhesión a las políticas de privacidad y procedimientos como pre-requisito de empleo.
- 

- ▶ Se impondra una multa civil de dinero a una entidad cubierta si se determina que la entidad ha violado una disposicion de simplificacion administrativa.
  - ▶ Se podra imponer una multa en la cantidad de mas de \$100 dolares por cada violacion o en exceso de \$25,000 para identicas violaciones durante un año calendario.
- 

- ▶ Para determinar la cantidad de penalidades se podrá considerar como factores agravantes o atenuantes, según corresponda, cualquiera de lo siguiente:
  - La naturaleza de la infracción, a la luz de la finalidad de la norma violada
  - Las circunstancias, incluyendo las circunstancias de violación incluyendo pero no limitado a:
    - El periodo de tiempo durante el cual se produjo la violación o violaciones
    - Si la violación causo daño físico
    - Si la violación obstaculiza o facilito la capacidad de un individuo para obtener atención de salud y
    - Si la violación resulto en daño financiero.

- ▶ El grado de culpabilidad de la entidad, incluyendo pero no limitado a:
    - Si la violación fue intencional y
    - Si la violación era fuera del control directo de la entidad.
  
  - ▶ Cualquier historial del previo cumplimiento de las disposiciones de la implicación administrativa, incluyendo violaciones, por la entidad incluyendo pero no limitado a:
    - Si la violación actual es igual o similar a violación previa.
    - Si hasta que punto la entidad ha intentado corregir las violaciones.
    - Como ha respondido a la asistencia técnica en el contexto del esfuerzo del cumplimiento
    - Como ha respondido a las quejas anteriores.
    - Si la entidad tiene problemas financieros que afecto su capacidad de cumplir
    - Si la imposición de multa pondría en peligro la capacidad de la entidad de seguir o pagar por el cuidado de salud.
- 

# “Security Breach”

- ▶ Un actuar fuera de una organización que omite o viola prácticas de políticas de privacidad, o procedimientos.
- ▶ Un acto interno similar se llama violación de seguridad.
- ▶ Ambas situaciones aunque diferentes se rigen a través de los derechos civiles y pueden tener penas iguales por violación desde multas hasta despidos y/o cancelación de contratos.

11 de abril de 2013

«PROV\_FNAME» «PROV\_MNAME» «PROV\_LNAME»  
«PROV\_ADDR1»  
«PROV\_ADDR2»  
«PROV\_CITY» «PROV\_STATE» «PROV\_ZIP»

Estimado(a) doctor(a):

El 13 de febrero de 2013 la Administración de Seguros de Salud del Estado Libre Asociado de Puerto Rico ("ASES") advino en conocimiento de una violación en el manejo de la información a la que la compañía CSA Architects & Engineers, PSC ("CSA"), entonces contratista de la ASES, tenía acceso como parte de la validación de datos del Health Information Technology Provider Incentive Program ("HITPIP"). Emitimos esta notificación en cumplimiento con nuestra obligación de garantizar la privacidad e integridad de su información y advertirle sobre el uso de la misma.

Esta violación ocurrió cuando un empleado de CSA, en contravención a las políticas de privacidad y seguridad de la ASES que venía obligado a cumplir, movió información que había sido provista por usted bajo el programa HITPIP sin contar con autorización para ello. La información involucrada en el incidente incluía su nombre y su código de identificación patronal para fines contributivos. Como resultado de esta situación el empleado de CSA fue despedido de su empleo, se le retiró de inmediato el acceso al sistema y a la información de la ASES, así como el acceso a nuestras facilidades. Además, el personal de CSA que ofrecía servicios en la ASES fue re-adiestrado en políticas de seguridad y privacidad en el manejo de información y se le restringió el acceso al sistema. Con posterioridad a estos eventos, la ASES y CSA han dado por terminada su relación contractual.

Tras la investigación de este evento no se han identificado datos que apunten al uso ilegal de su información. Sin embargo, de usted tener alguna pregunta relacionada a esta notificación y al evento a aquí descrito puede comunicarse libre de costo al 1-800-981-2737 de lunes a viernes entre 8:00 a.m. y 4:30 p.m.

En la ASES estamos comprometidos con la protección de su información y continuaremos trabajando para garantizar el manejo adecuado de la misma y la seguridad de nuestros sistemas.

Cordialmente,



William Ruiz Alejandro  
Oficial de Privacidad

11 de abril de 2013

«First\_Name»  
«Address\_Line\_1»«Address\_Line\_2»  
«City» «State» «ZIP\_Code»

Estimado paciente:

El 13 de febrero de 2013 la Administración de Seguros de Salud del Estado Libre Asociado de Puerto Rico ("ASES"), advino en conocimiento de una violación en el manejo de su información de salud por parte de la compañía CSA Architects & Engineers, PSC ("CSA"), entonces contratista de la ASES. Aunque la información de salud involucrada en este incidente está codificada, emitimos esta notificación en cumplimiento con nuestra obligación de garantizar la privacidad e integridad de su información y mantenerle informado(a) del uso y manejo de la misma.

Esta violación ocurrió cuando un empleado de CSA, en contravención a las políticas de privacidad y seguridad de la ASES que venía obligado a cumplir, movió información de salud de manera no autorizada. La información involucrada en el incidente incluía su nombre y el código de procedimiento ordenado por su proveedor de servicios médicos. Como resultado de este incidente el empleado de CSA fue despedido de su empleo, se le retiró de inmediato el acceso al sistema y a la información de la ASES, así como el acceso a nuestras facilidades. Además, el personal de CSA que ofrecía servicios en la ASES fue re-adiestrado en políticas de seguridad y privacidad en el manejo de información y se le restringió el acceso al sistema.

Tras la investigación de este evento no se han identificado datos que apunten al uso ilegal de su información. Sin embargo, de usted tener alguna pregunta relacionada a esta notificación y al evento a aquí descrito puede comunicarse libre de costo al 1-800-981-2737 de lunes a viernes entre 8:00 a.m. y 4:30 p.m.

En la ASES estamos comprometidos con la protección de su información y continuaremos trabajando para garantizar el manejo adecuado de la misma y la seguridad de nuestros sistemas.

Cordialmente,



William Ruiz Alejandro  
Oficial de Privacidad

# PROCOLOS

# Información Mínima Necesaria

1

- Utilizar el mínimo necesario para realizar funciones de trabajo
- De no estar seguro sobre el nivel de acceso, consultar con su supervisor o Director.

2

- No divulgar información que no haya sido preguntada
- No solicitar información más allá de la necesaria para realizar el trabajo.

3

- Utilizar la experiencia y juicio profesional para divulgar información
- De necesitar enviar un fax seguir los procedimientos establecidos
- En caso de duda a los procedimientos o políticas de privacidad consultar .

# Llamadas Realizadas a Beneficiarios

1

- Del beneficiario no estar disponible, dejar solamente, Nombre, número de teléfono donde el beneficiario pueda comunicarse.
- De tener algún problema de Lenguaje o incapacidad el beneficiario, debe solicitar que un tercero obtenga el permiso para comunicarse..

2

- Del beneficiario no encontrarse y tener una contestadora de teléfono, solamente dejar nombre, nombre del beneficiario a quien va dirigido el mensaje, solicitud de que le devuelva llamada y un numero de teléfono.

3

- No se debe comunicar vía telefónica, información psiquiátrica, información relacionada a Abuso y/o tratamiento de drogas y alcohol, información sobre violencia domestica y diagnósticos de VIH

# Manejo de Documentos

1

- Asegurar que los documentos tienen la información necesaria para cumplir con el propósito para el cual es enviado
- Verificar que la hoja de fax tenga la advertencia de confidencialidad

2

- Verificar que la persona a la que se le envíe el fax esté al tanto del envío de los documentos.
- Comunicarse con el recipiente del fax para verificar que llegó

3

- En caso de error al enviar el fax, comunicarse con la persona que lo recibió por error y solicitar la destrucción de los documentos
- Una vez se envíe el fax, iniciar y archivar la hoja de trámite en el lugar correspondiente.

# Seguridad Física

1

- Los documentos deben estar guardados al final del día bajo llave en un lugar seguro.
- Al tirar a la basura asegurarse que el documento no tenga información de salud y triturarlo antes de tirarlo a la basura.

2

- Evitar dejar documentos que contengan información de salud de los beneficiarios sobre el escritorio ni visible a otras personas.
- Al imprimir un documento buscarlo tan pronto lo imprima.

3

- Utilizar “screen savers” cuando no se esté trabajando con la computadora.
- No comunicar o dejar su contraseña o nombre de usuario en un lugar de fácil acceso.
- Verificar que la computadora quede apagada al finalizar el día.
- Las conversaciones con los beneficiarios deben ser confidencial.

- ▶ Este es un trabajo de todos para cuidar de la Información de Salud Protegida para beneficio de nuestros Beneficiarios de Mi Salud y de los Proveedores, al igual que para Nuestra Agencia.
- ▶ Así que debemos crear conciencia sobre la importancia que tenemos en nuestras manos de cómo manejamos la información recibimos y divulgamos y como velamos por cumplir las Reglas de Privacidad y Seguridad.