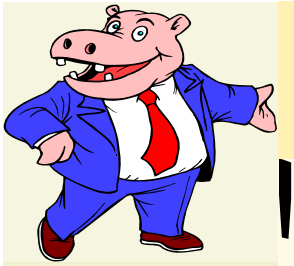


Volumen 1 Núm. 1
Septiembre-Octubre 2002
Autorizado por la Comisión Estatal de Elecciones

First Point Healthcare Group Inc.
Oficina de Privacidad y Seguridad HIPAA
Departamento de Salud

"TODO sobre HIPAA"

Análisis y Asesoramiento sobre Privacidad, Confidencialidad, Códigos y Transacciones

ADENTRO

MENSAJE DEL SECRETARIO DE SALUD

Hon. Johnny Rullán *M.D. FAC PM*

LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN DE SALUD

En el campo de la salud el asunto de la privacidad, confidencialidad y seguridad de la información de salud del paciente es, junto a la calidad del tratamiento, el asunto principal a considerar en la prestación de servicios. Esto incluye a todo proveedor de servicios de salud, médicos, farmacias, laboratorios, terapistas, hospitales, aseguradoras, "nursing homes", "clearinghouses", gobierno federal, gobierno estatal, municipal, etc., etc., etc. Cuando el Congreso de los Estados Unidos aprobó el Health Insurance Portability and Accountability Act del 1996, conocida como la ley HIPAA, se pusieron en marcha cambios significativos en la prestación de los servicios de salud que a la larga tendrán un impacto enorme en la práctica de la medicina, en la relación médico-paciente y en las finanzas de la industria de la salud en su totalidad.

Continúa en la página 2

ALERTA!!! ALERTA!!! ALERTA!!!

- El martes **15 de octubre de 2002** , es la fecha límite para someter la solicitud de prórroga al Departamento de Salud Federal para cumplir con las disposiciones sobre códigos y transacciones uniformes de la ley HIPAA.
- La solicitud debe incluir el plan de la entidad para el cumplimiento al **16 de octubre de 2003**. No obstante, se requiere que las pruebas de cumplimiento se realizen para el **16 de abril de 2003**.
- El lunes **14 de abril de 2003**, entran en vigor las reglas sobre privacidad y confidencialidad de la Información de Salud del Paciente de HIPAA. A esa fecha las entidades cubiertas deberán haber establecido los nuevos formularios, notificaciones, procesos, y procedimientos que requiere la ley.
- No olvide que los nuevos formularios, notificaciones, procesos y procedimientos deberán incluir lo dispuesto por las leyes de Puerto Rico aplicables junto a HIPAA (Ej. Carta de Derechos y Obligaciones del Paciente, Salud Mental).
- Para el **14 de abril de 2003** todo el personal, incluyendo voluntarios, médicos, profesionales de la salud, administradores, empleados a tiempo parcial, etc. deberán haber sido debidamente adiestrados sobre HIPAA y las leyes de Puerto Rico que protegen la privacidad y confidencialidad de la información de salud del paciente.
- El cumplimiento con las reglas de Asociados de Negocio se extendió al **14 de abril de 2004** para aquellos contratos que venzan luego de esa fecha. Los que venzan después del **14 de abril de 2003** deberán renovarse cumpliendo con las reglas.
- El **31 de diciembre de 2003** Medicare dejará de recibir facturación en forma manual.▲

LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN DE SALUD

Estos cambios tienen que ver con tres grandes áreas:

1. La uniformidad de las transacciones electrónicas y códigos en la industria.
2. La privacidad y confidencialidad de la información de salud del paciente.
3. La seguridad de la información de salud, tanto almacenada como transmitida electrónicamente, en papel, u oral, ya sea pasada, presente y/o futura.

Para efectos de las reglas de privacidad de HIPAA, un proveedor de servicios de salud está cubierto por las mismas, y será considerado como una **entidad cubierta**, si en algún momento ese proveedor de servicios transmite información de salud por medios electrónicos relacionada con una de cualquiera de las transacciones cubiertas por la ley. Además, el proveedor de servicios de salud también estará sujeto a las reglas sobre privacidad a través de las disposiciones que tienen que ver con lo que la ley llama **asociados de negocio**. HIPAA no incluye a aquellos proveedores de servicios de salud que no usen transmisión electrónica en ninguna de las transacciones cubiertas por la ley. Aquel que lo haga todo en papel no estará sujeto a las reglas de HIPAA. No obstante, aquel que use medios electrónicos para transmitir información de salud, aunque sea en una sola ocasión, estará sujeto a las reglas de privacidad de HIPAA que aplicarán, no sólo a la información transmitida electrónicamente, sino a la que mantiene en papel o comunica verbalmente.

Las transacciones electrónicas cubiertas por las reglas de privacidad y seguridad son las siguientes:

1. Información sobre cualquier reclamación de servicios de cuidado de salud o cualquier encuentro equivalente.
2. Pago de servicios de salud o solicitud de envío del pago.
3. Coordinación de beneficios.
4. Informes sobre el estatus de reclamación de servicios de cuidado de salud.
5. Registro o dado de baja de registro en cualquier plan de salud.
6. Elegibilidad del plan de salud.
7. Pago de primas del plan de salud.
8. Certificación y autorización de referido.
9. Primer informe sobre un accidente o condición médica.
10. Los documentos que acompañan a una reclamación de servicios de salud.
11. Cualquier otra transacción que el Departamento de Salud Federal disponga por reglamentación.

Las reglas de privacidad sólo aplican a **información de salud protegida (PHI)** que se define como cualquier información de salud que identifique a la persona a la que se refiere y que sea transmitida electrónicamente o mantenida en papel por una entidad cubierta por la ley.

Las últimas enmiendas a las reglas de privacidad de HIPAA eliminaron el consentimiento para tratamiento, pago o cualquier otra operación para el cuidado de la salud (TPO), sustituyéndolo por el evidenciar la notificación al paciente de la política de privacidad y confidencialidad de la entidad. No obstante, la Carta de Derechos y Obligaciones del Paciente de Puerto Rico, Ley Número 194 del 25 de agosto de 2000, requiere el consentimiento para tratamiento, pago y otras operaciones de salud, prevaleciendo en este aspecto sobre HIPAA.

Por otro lado, para divulgar información la entidad cubierta debe hacer todo esfuerzo razonable para **limitarla al mínimo necesario** para que la información sirva el propósito para lo que se solicita. El riesgo de equivocarse al divulgar información demás lo asume la entidad.

No existe el **requerimiento de mínimo necesario** cuando se trata de requerimientos o solicitud de información relacionada con el tratamiento del paciente o cuando sea al propio paciente.

Otro requerimiento de HIPAA es que la **entidad cubierta** entre en contratos escritos con sus **asociados de negocio** antes de que pueda **compartir información de salud protegida (PHI)** con ellos. La definición de **asociados de negocio** podría incluir consultores, abogados, actuarios, contables, administradores, compañías o asociaciones de acreditación, de servicios financieros, de administración o de facturación. Lo importante no es el título sino el que la persona u organización contratada tenga acceso a información de salud protegida del paciente (PHI). Una **entidad cubierta,** podría a su vez ser **asociado de negocio** de otra **entidad cubierta**.

Un contratista independiente con el que no exista un contrato como **asociado de negocio** podría ser tratado como empleado de la **entidad cubierta**. Los empleados o la **fuerza trabajadora** pueden estar expuestos a sanciones bajo HIPAA, no así los **asociados de negocio**. Por **fuerza trabajadora** se entiende empleados, voluntarios, personas bajo adiestramientos y cualquier otro que esté y trabaje bajo el control de la entidad.

Los contratos con los asociados de negocio requieren, entre otras cosas: (a) disposiciones sobre el uso permitido y la divulgación de la información a terceros por parte del asociado, (b) la protección de la información por parte del asociado, (c) hacer disponible sus libros, récords y prácticas internas al Departamento de Salud de los Estados Unidos para determinar si está cumpliendo con la regla de privacidad, (d) devolver o destruir la información protegida (PHI) al finalizar sus servicios, y (e) si el asociado contrató a terceros que recibirán la información, estos últimos deberán proteger la misma igual que el asociado.

Por otro lado, las reglas de privacidad de HIPAA modifican el concepto de **autorización**. Esto significa que la entidad cubierta tiene que obtener una **autorización explícita** del paciente antes de divulgar información de salud protegida (PHI) para otros propósitos que no sean tratamiento, pago u otras operaciones de salud (TPO). Por tanto, la autorización se utiliza para divulgación que no tiene que ver con tratamientos, pagos u otras operaciones de salud, mientras que el consentimiento se limita precisamente a estas tres. Las condiciones de cada autorización podrían variar dependiendo de la situación y los pacientes tienen el derecho de revocar una autorización ya dada o limitarla a determinado período de tiempo o propósito. No obstante es importante notar que la Carta de Derechos y Obligaciones del Paciente de Puerto Rico solo permite la divulgación de la información de salud para otros propósitos que no sean tratamiento, pago u otras operaciones de salud mediante orden judicial. En eso, también difiere y es más estricta que HIPAA. Por tanto en Puerto Rico es necesario considerar la Carta de Derechos y Obligaciones del Paciente al implantar HIPAA.▲

Sobre la Oficina de Privacidad y Seguridad HIPAA

El Secretario de Salud, mediante la Orden Administrativa Número 170, adoptó como política pública del Departamento de Salud y todas las agencias y entidades de la Sombrilla, el propósito, requerimientos y metas de la ley HIPAA. Para asegurar la implantación y el cumplimiento subsiguiente con la referida ley, esta Orden crea un Comité Timón. Este Comité estará compuesto por los Oficiales de Privacidad y Seguridad que sean nombrados por las entidades cubiertas parte de la sombrilla. Su función principal será facilitar y fiscalizar la implantación, administración y el cumplimiento de toda la reglamentación de la Ley HIPAA aplicable a las entidades cubiertas en la sombrilla de salud. En términos de operación y funcionalidad este Comité ejercitará sus funciones a través de la Oficina de Privacidad y Seguridad HIPAA (OPSH) que estará dirigida por el Oficial Principal de Privacidad y Seguridad que nombre el Secretario de Salud. Entre sus funciones principales podemos mencionar: **1)** Ayudar a la directiva de cada "entidad cubierta" al establecimiento del Comité Coordinador en cada una de las Agencias de la Sombrilla, **2)** Servir como organismo consultor en materia de privacidad y seguridad de la información para todos los departamentos y entidades apropiadas, **3)** Velar para que todas las instituciones, públicas o privadas que están cobijadas por el Departamento de Salud cumplan al día con los estándares establecidos por la Ley HIPAA y su reglamentación, y **4)** Mantener informado al Secretario de Salud del estado de desarrollo de la implantación de la ley HIPAA en cada una de sus Agencias. Deberá informar asimismo de su cumplimiento posterior. Para realizar sus funciones se le ha otorgado a este Comité: Poder de Convocación y Poder para Solicitar Producción de Documentos sobre todos y cada uno de los organismos bajo la sombrilla. En este momento estamos trabajando, por designaciones administrativas, con excelentes funcionarios que están dando de su tiempo por el bien del Departamento. Pronto se estará implantando formalmente la estructura de trabajo que dedicará todos sus esfuerzos a la implantación y cumplimiento de la ley para el beneficio de todos nuestros pacientes.▲

Las sanciones por violaciones a la Ley HIPAA

Las sanciones por violaciones a esta ley son de tres tipos, civiles, penales y administrativas. El Departamento de Salud de los Estados Unidos delegó en su Oficina de Derechos Civiles lo relativo a la imposición de sanciones. Además, las entidades cubiertas por la ley deberán desarrollar su propio sistema de **sanciones administrativas internas para "su fuerza trabajadora" y sus "asociados de negocio"** que violen la ley, sanciones que podrían llegar hasta despido o la cancelación del contrato, según sea el caso. Las penalidades civiles y criminales son las siguientes:

1. No cumplir con los estándares desde **$100 por persona por violación hasta $25,000 por persona por violación de un sólo estándar** en un año calendario.
2. Por el **uso y divulgación indebida de información de salud protegida o por la obtención de esa información, hasta $50,000 de multa y un año de prisión.**
3. Si la violación anterior es cometida **bajo fraude o engaño** la penalidad sería de **$100,000 de multa y hasta cinco (5) años de cárcel.**
4. Si la violación es **con el propósito o intención de vender**, **transferir, o usar información de salud protegida identificable con el propósito de obtener ventajas comerciales o de negocio, ganancias personales o causar daño malicioso, la pena podría ser de hasta $250,000 dólares de multa o 10 años de cárcel.**

Además, hay que dejar claro que HIPAA no crea una acción legal por daños a favor del paciente. Pero bajo las leyes de Puerto Rico el paciente podría considerarse un tercero beneficiario o tener una causa de acción bajo las leyes de protección del consumidor o de privacidad estatales, utilizando las normas y estándares de HIPAA. En el caso de Puerto Rico la situación es aún más clara en términos del derecho a demandar por violaciones a la privacidad, ya que la protección de la dignidad, del ser humano y su derecho a la privacidad está consignado en la Constitución. Carta de Derechos, Art. II, Sec.1.

Por otro lado, HIPAA requiere que las entidades cubiertas por la ley establezcan sanciones disciplinarias contra aquellos empleados que la violen. Estas sanciones pueden llegar hasta el despido. Esto requiere que la Oficina de Recursos Humanos se envuelva en el proceso de implantación de la ley.

Además, se le requiere a la entidad cubierta tomar aquellas medidas disciplinarias contra los asociados de negocio que violen la ley.▲

LA CARTA DE DERECHOS Y OBLIGACIONES DEL PACIENTE

En el año 2000 Puerto Rico legisló para crear la Carta de Derechos y Responsabilidades del Paciente, Ley Núm. 194 del 25 de agosto de 2000. En el año 2001 se amplió esta legislación con la creación del cargo del Procurador del Paciente para los pacientes beneficiarios de la Reforma de Salud, Ley Núm. 11 del 11 de abril de 2001. La propia ley dispone que en cinco años se extenderá la legislación a todos los pacientes de salud.

La Ley 194 establece en su exposición de motivos los asuntos que quiere reglamentar y los derechos que quiere proteger. Se pueden resumir en los siguientes:

1. Acceso adecuado a servicios de salud de calidad como un derecho fundamental.

2. Acceso y libre flujo de información **completa, fidedigna y veraz** a los usuarios y consumidores de servicios de salud.

3. Penalizar a aquéllos proveedores y aseguradores de servicios de salud que violen la ley al no divulgar la totalidad de la información que se le requiere divulgar, o intencionalmente o a sabiendas, divulgar información falsa.

Esta ley incluye a todas las facilidades y servicios de salud médico-hospitalarios, profesionales de la salud, aseguradoras y planes de cuidado de salud. Protege a todos los usuarios y consumidores de tales servicios y facilidades, irrespectivamente de la naturaleza pública o privada del proveedor o de cualquier otra condición o consideración.

Los derechos que la ley concede a los usuarios son los siguientes:

1. Recibir **servicios de salud de la más alta calidad** consistente con los principios generalmente aceptados en la práctica de la medicina.

2. Recibir información **cierta, confiable, oportuna, de fácil comprensión y adecuada a sus necesidades** con relación a su (a) plan de seguro de salud; (b) facilidades y profesionales de la salud; (c) beneficios cubiertos por el plan; (d) costo de las primas y deducibles; (e) mecanismos y procedimientos de recobro de costos y solución de disputas; (f) localización de facilidades y profesionales; (g) mecanismos y procedimientos de control de calidad y garantías de satisfacción; (h) procedimientos de acceso a especialistas y servicios de emergencia e (i) las reglas y procedimientos para el manejo o administración del cuidado de la salud.

3. Recibir **información adecuada y suficiente** sobre (a) educación, (b) licenciamiento, (c) certificación, (d) re-certificación y (e) experiencia del profesional de la salud; (f) su experiencia en el procedimiento a llevar a cabo; (g) alternativas razonables de tratamiento, (h) costo de los mismos y sus probabilidades de éxito; (i) e información sobre los mecanismos y procedimientos de control de calidad.

4. Recibir **información adecuada y suficiente** relativa (a) al personal y los recursos técnicos disponibles para llevar a cabo los procedimientos y (b) la educación, preparación y experiencia del personal que los realizará.

5. Selección de planes y proveedores adecuada y suficiente para garantizar servicios de alta calidad; que los servicios cubiertos por el plan estarán accesibles, sin demoras irrazonables y en razonable proximidad geográfica; acceso a emergencias 24 horas al día, 7 días a la semana y acceso a especialistas según los procedimientos de referido conforme al plan. Si se requiere autorización especial bajo el plan para el acceso a especialistas el plan garantizará un número adecuado de visitas.

6. Continuidad de los servicios si se cancela o termina un plan o se cancela un proveedor (notificación con 30 días de anticipación) y la continuación del plan por 90 días sujeto al pago.

7. Participación en la toma de decisiones sobre el tratamiento.

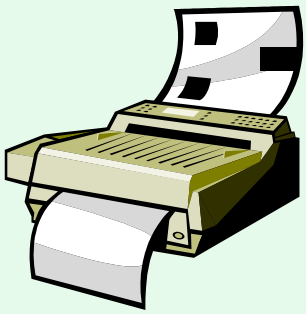
8. Respeto y trato igual.

La ley regula además, el uso y divulgación de la información de salud del paciente, garantizándole libre acceso, copia del mismo, comunicación, confidencialidad y estricta privacidad. **Su información no puede ser divulgada sin su autorización escrita y sólo para fines de tratamiento, prevención, control de calidad o pago de servicios. La divulgación no autorizada sólo se hará por orden judicial previa o por disposición de ley. Por último, la ley establece un procedimiento de quejas y agravios.▲**

Concluye el análisis de deficiencias del Departamento de Salud

First Point Healthcare Group terminó el análisis de deficiencia para cumplimiento con HIPAA del Departamento de Salud y las agencias de su sombrilla. Como parte del análisis se adiestró a sobre ochocientos empleados de nivel intermedio. Como parte de esta fase se radicaron las solicitudes de prórroga para cumplir con la parte de códigos y transacciones. Próximamente comenzará la implantación.▲

El uso del facsímil y la protección de la información de salud del paciente bajo HIPAA



Aunque el facsímil no está incluido entre aquellos instrumentos de transmisión de información electrónica reglamentados bajo la ley HIPAA, su mal uso o su inadecuada reglamentación puede dar lugar a que información de salud del paciente protegida sea divulgada inadecuadamente en violación a la misma.

Su entidad puede transmitir información de salud protegida del paciente utilizando el facsímil. Dicho envío no está prohibido ni reglamentado por HIPAA. Lo que su entidad, o usted no puede hacer es permitir o actuar en tal forma que la información transmitida usando el facsímil sea divulgada de forma inadecuada y en violación a la ley.

A continuación sugerimos algunas normas y procedimientos que la entidad cubierta podría utilizar para reglamentar la transmisión de información de salud del paciente usando este instrumento.

En cuanto a la máquina de facsímil:

1. Separe las máquinas de facsímiles para uso regular de la oficina de aquellas que se utilizan para transmitir y/o recibir información de salud protegida del paciente. Así se evita que información de salud protegida sea, por inadvertencia, recogida y circulada junto a información rutinaria de la oficina.

En cuanto a la transmisión de la información de salud:

1. Desarrolle una hoja para la transmisión de los facsímiles que específicamente haga referencia a la información de salud transmitida y su protección bajo la ley. El título de la hoja de envío debe leer en letras grandes de la siguiente forma: **"Esta Transmisión Incluye Información Confidencial de Salud".** Inmediatamente debajo del título anterior sugerimos el siguiente texto:

"La información transmitida es para el uso exclusivo de la persona o entidad a la que va dirigida. Incluye información de salud que es personal y sensitiva. Esta información es una de naturaleza privilegiada y confidencial. Ha sido transmitida luego de haberse recibido la autorización del paciente o bajo circunstancias que no requieren su autorización.

La persona a quien va dirigida la información tiene la obligación de mantenerla segura, protegida y confidencial. El divulgar esta información a terceros sin autorización adicional del paciente o de acuerdo a lo que permite la ley está <u>totalmente prohibido</u>. El hacerlo puede traer como consecuencias penalidades severas de tipo civil y/o criminal bajo las leyes federales y estatales.

Si la persona que recibe o lee esta información no es la **persona a la que está dirigida la misma, o el empleado o agente responsable de hacer llegar la misma a esa persona, se le notifica y advierte que cualquier divulgación, diseminación, distribución o fotocopia de la misma está <u>total y estrictamente</u> prohibida, tanto por la ley federal como la estatal.**

Si usted ha recibido esta información por error, favor de notificarnos y destruir la misma lo más pronto posible".

2. Incluya además, en la hoja de transmisión del facsímil, la siguiente información:

- Fecha y hora de envío
- Nombre, dirección, número de teléfono y facsímil de quien lo envía
- Nombre, dirección, teléfono y facsímil de la persona a quien está dirigida la información
- Número de páginas transmitidas
- Información para verificar el recibo del facsímil.

En cuanto a la información de salud a ser transmitida:

1. Antes de transmitir información de salud del paciente vía facsímil, asegúrese de que cuenta con una autorización de éste en su expediente para transmitirla utilizando ese medio.

2. Limite el uso del facsímil a situaciones urgentes o no rutinarias cuando el envío por correo o mensajero no es aconsejable o posible.

3. Evite transmitir información sensitiva sobre la salud del paciente utilizando el facsímil. Por ejemplo, información sobre dependencia a las drogas, enfermedades transmitidas sexualmente, HIV, o cualquier otra información de carácter muy personal.

4. Recuerde que bajo la Ley de Salud Mental de Puerto Rico, Ley Número 408 del 2 de octubre de 2000, no se puede transmitir información de salud mental del paciente usando el facsímil sin su <u>autorización expresa</u> (Artículo 2.14). Evite utilizar el facsímil hasta donde sea ello posible para enviar dicha información. Para prever, en caso de que en una emergencia tenga que utilizar el facsímil para enviar dicha información, prepare y obtenga una autorización expresa del paciente para la transmisión de información sobre su salud mental vía facsímil.

5. Cuando esté esperando un facsímil con información de salud de un paciente, coordine con la persona que lo enviará para evitar que el mismo permanezca mucho tiempo en la máquina sin ser recogido.

6. En caso de que vaya a recibir un volumen grande de facsímiles conteniendo información de salud protegida del paciente (PHI), designe empleados autorizados para recibir y distribuir los mismos.

7. Al igual que con cualquier otra información de salud protegida, no importa cómo la haya recibido, asegúrese de que los facsímiles sean colocados en un lugar seguro y confidencial cuando son entregados.

8. Confirme siempre que los números de facsímil a donde enviará la información sean los correctos. Asegúrese además de la seguridad de la máquina de facsímil de la persona a quien va dirigido. Llámelo y notifíquele que estará enviando un facsímil. Requiérale que le verifique el recibo del mismo. No confíe ni dependa de números de facsímil listados en guías. ▲

Sobre los derechos del paciente bajo HIPAA

- Los derechos básicos relacionados con la información de salud del paciente que la ley federal protege y que deben ser informados a éste en forma simple y sencilla son:
  * El derecho a ser notificado con la Poítica de Privacidad y Confidencialidad de la entidad.
  * El derecho a tener acceso a su información de salud protegida.
  * El derecho a ser notificado del número de veces que su información de salud ha sido divulgada.
  * El derecho a requerir cambios en su información de salud si ésta no es precisa, cierta o no está completa.
- La regla también provee para que familiares y amigos del paciente, bajo determinadas circunstancias, tengan acceso a información protegida de éste. Hay que señalar que la información de salud protegida del paciente continúa siendo protegida aún después de la muerte del paciente y estos derechos son heredados por su sucesión.
- Para proteger la información de salud del paciente que cae bajo la protección de la Ley HIPAA, se requiere que los proveedores establezcan nuevas políticas y procedimientos y que designen un oficial de privacidad responsable de recibir todas las querellas. También se requiere el adiestramiento de todo el personal de la entidad sobre la Ley HIPAA que debe ser complemento del programa de cumplimiento con la ley. Esto incluye tanto el personal existente como nuevo personal al ser reclutado. Por último, para cumplir con las reglas de privacidad, el proveedor o **entidad cubierta** debe poner en vigor aquellas salvaguardas de seguridad física, administrativas y técnicas relacionadas al almacenaje, acceso y transmisión de la información que sean necesarias para protegerla. Las reglas finales de seguridad de HIPAA complementarán las de privacidad.
- Por último, las reglas de privacidad de HIPAA establecen un proceso para hacer no identificable la información de salud protegida (PHI). Esto se hace eliminando de la información ciertos identificadores del paciente. La información sin identificación puede ser divulgada, pero aún así sujeta a ciertas condiciones.▲

¿Sabía usted que …???

* Al desarrollar e implantar un programa para el adiestramiento del personal de su empresa debe hacerlo en forma amplia, de forma tal que cubra no sólo lo que dispone HIPAA, sino además, las leyes de Puerto Rico que protegen la privacidad y confidencialidad de la información de salud del paciente. Su organización tiene que cumplir tanto con HIPAA como con las leyes de Puerto Rico aplicables. En algunos casos, tiene que cumplir con algunas disposiciones de HIPAA y con otras disposiciones de las leyes de Puerto Rico a la misma vez. Esto es, la propia ley HIPAA lo obliga a tener que cumplir, no sólo con ella, sino con la legislación local en aquellas disposiciones o normas donde ésta es más estricta.

* El adiestramiento de su fuerza trabajadora que requiere HIPAA incluye a todo el personal, tanto a tiempo completo como a tiempo parcial, incluyendo empleados temporeros y voluntarios. El mismo debe cubrir la política de privacidad y confidencialidad de su empresa y sus consecuencias en términos de las responsabilidades de cada posición. Los nuevos empleados deben ser adiestrados como parte de su orientación. Además, cada vez que cambie su política o que se hagan cambios en la ley o en las reglas de privacidad, deberá adiestrar aquellos empleados cuyas funciones, deberes y obligaciones se afecten.

* Debe documentar los adiestramientos que realiza y mantener récord de ellos al menos por seis (6) años. Su oficina o oficial de privacidad deberá conservar estos récords, además de guardar copia en el expediente de personal de cada empleado.

* Al adiestrar a un proveedor, enfoque el adiestramiento en los derechos del paciente y en la obligación de respetar los mismos y no en las reglas. Explíqueles las consecuencias que les traerá el no cumplir con estas obligaciones. Prepare un listado con aquellos puntos principales que debe recordar al manejar la información de salud protegida. Deje el adiestramiento detallado para el administrador de la oficina, quién es el responsable de lograr los cambios de conducta necesarios en la entidad.

* No basta con desarrollar un acuerdo especial para sus asociados de negocios. El Departamento de Salud Federal no se ha expresado con claridad sobre hasta que punto se extenderá su supervisión de la relación entidad cubierta–asociado de negocios. Por ello es necesario comenzar a establecer mecanismos para evaluar al asociado de negocio. Una especie de "due diligence" de su operación. Por ejemplo, es importante saber si el asociado:
  - Tiene una póliza de seguro que cubra errores y omisiones, responsabilidad general o que cubra las facilidades de la empresa.
  - Ha firmado acuerdos de asociados de negocio con otras entidades.
  - Tiene un oficial de seguridad o privacidad.
  - Tiene procedimientos establecidos sobre divulgaciones, acceso o enmiendas a la información de salud.
  - Divulga información de salud a terceros.
  - Tiene un programa de adiestramiento sobre privacidad y/o seguridad.
  - Tiene procedimientos para devolver o destruir la información.▲

Sobre los Asociados de Negocios

La mayoría de las organizaciones requieren la asistencia de contratistas, consultores, vendedores, proveedores de servicio u otro personal externo a la misma para poder llevar a cabo sus actividades regulares. Estos "asociados de negocios", como los denomina la ley HIPAA en sus reglas de privacidad, **son aquellas personas o entidades que llevan a cabo funciones, actividades o servicios para la organización y que el proceso envuelve en alguna forma el uso o divulgación de información de salud protegida de los pacientes.**

Determinar quién es un "asociado de negocios" bajo HIPAA puede ser difícil. El criterio para determinar si lo es o no es si dicha persona o entidad tiene acceso a información de salud protegida del paciente (PHI).

Veamos varios casos o situaciones particulares:

- Un servicio de limpieza no tiene por qué accesar o divulgar información de salud protegida de pacientes de la entidad cubierta. No obstante, si durante el trabajo día a día de dicho servicio de limpieza en forma regular y contínua la información de salud de los pacientes está accesible a dicho servicio, la entidad cubierta estaría violando las disposiciones de HIPAA sobre privacidad si no protege la misma. En esta situación la entidad cubierta debe considerar al servicio de limpieza un asociado de negocio y firmar con ellos un contrato de asociado de negocios siguiendo lo dispuesto por HIPAA. No obstante, por lo regular no se considera un Asociado.
- Un abogado que rinde sus servicios a una entidad cubierta podría ser o no un asociado de negocios. Por ejemplo, un abogado asesor en asuntos laborales que no tiene acceso a información de salud de los pacientes de la entidad cubierta no es un asociado de negocios. No obstante los servicios legales que provee el abogado que representa a la entidad cubierta en casos por mala práctica médica lo coloca en situación de tener que accesar información de salud protegida de pacientes lo que lo convierte en un asociado de negocios de ésta.
- Un hospital que le provee los servicios de facturación y cobro a un grupo de práctica médica es, además de una entidad cubierta, también un asociado de negocios en cuanto a dicho grupo médico.
- Una entidad que provee servicios de codificación, facturación y/o cobro a un laboratorio, un grupo de terapistas físicos o a un grupo de médicos cubierto es su Asociado de Negocio.
- Algunos de los servicios o entidades que podrían ser consideradas como asociados de negocios son:
  - ∗ Agencias de facturación y cobro
  - ∗ Servicios de seguridad bajo determinadas circunstancias
  - ∗ Agencias de cobro
  - ∗ Abogados
  - ∗ Contables
  - ∗ Auditores
  - ∗ Servicios de transcripción
  - ∗ Vendedores de "software"
  - ∗ Vendedores de "hardware"
  - ∗ Servicios de almacenamiento de documentos
  - ∗ Servicios de disposición de documentos
  - ∗ Servicios de administración
  - ∗ Servicios clínicos
  - ∗ Servicios de reparación de fotocopiadoras, equipo de rayos X, equipo de laboratorio, etc.
  - ∗ Servicios de mensajería bajo determinadas circunstancias y condiciones.▲

Noti-HIPAA

- ♦ Las propuestas enmiendas de las Reglas de Privacidad y Confidencialidad, anunciadas el pasado mes de marzo, eliminan la necesidad de obtener el consentimiento del paciente antes de tratarlo.
- ♦ First Point llevará a cabo la implantación de HIPPA para la Sociedad de Educación y Rehabilitación de Puerto Rico (SER de Puerto Rico), una afiliada de Easter Seals de los Estados Unidos.
- ♦ Se espera que durante este mes de octubre el Departamento de Salud Federal publique las reglas finales de seguridad de HIPAA.
- ♦ La Universidad Interamericana y First Point han preparado un programa de educación continuada con créditos para los profesionales de salud sobre la ley HIPAA y otras leyes de Puerto Rico que protegen los derechos del paciente. El mismo consta de un curso de treinta (30) horas y dos (2) cursos especializados de veinte (20) horas cada uno. Los participantes se convertirán a su vez en adiestradores del personal de sus empresas y podrán desempeñar en algunos casos el puesto de Oficial de Privacidad de la empresa. El curso de treinta (30) horas es para todo el personal. Los cursos especializados de veinte (20) horas cada uno serán para personal de informática uno y para proveedores el otro. Estos se ofrecerán utilizando las técnicas de teleconferencia en ocho recintos a través de toda la Isla.
- ♦ La implantación de la Ley HIPAA requiere el incorporar en dicho proceso las leyes de Puerto Rico que son más estrictas ("stringent") que continúan aplicando en forma complementaria o que continúan aplicando porque HIPAA las incluye en aquellas estatales que continuarán vigentes.
- ♦ El Departamento de Salud como agencia licenciadora y evaluadora de facilidades de salud, laboratorios, farmacias, profesionales de la salud y médicos será responsable de velar porque se implante adecuadamente la ley HIPAA en esas instituciones.▲

Mitos y Realidades sobre HIPAA

MITO: Hay que guardar los récords de los pacientes bajo llave.

HIPAA: Sólo **asegurar** los récords.

REALIDAD: Esto no quiere decir bajo llave. Existen alternativas razonables.

MITO: Hay que hablar en un lugar donde otros no puedan escuchar la conversación entre el profesional y el paciente.

MITO: Hay que construir lugares a prueba de sonido.

MITO: Tengo que construir e instalar barreras de sonido en mis topes o "counters".

HIPAA: Falso, sólo tomar medidas razonables para mantener la privacidad de la información de salud del paciente.

REALIDAD: Esto quiere decir, bajar el volumen, ir a una esquina a conversar si hay otras personas en el lugar, pedir a los visitantes que le permitan hablar en privado, atender a una persona a la vez, hablar en otro tono de voz, etc.

MITO: Tienes que comprar un programa de computadoras.

HIPAA: Falso, entre otras cosas, hay que elaborar una política de privacidad, la documentación y procedimientos necesarios para cumplir con las reglas y adiestrar todo el pesonal de la entidad.

REALIDAD: Se puede cumplir completamente con HIPAA sin comprar nada nuevo.

MITO: Existen programas de computadoras certificados y/o que llevan a cumplir con HIPAA automáticamente.

HIPAA: Falso, los únicos que pueden cumplir con HIPAA son planes, proveedores y "clearinghouses".

REALIDAD: No existe programa en el universo que esté certificado por o para HIPAA, ni que lo haga cumplir con HIPAA automáticamente. Lo más que pudieran es ser "conformes" con HIPAA.

MITO: Puedes ir a la cárcel si no cumples con HIPAA

HIPAA: Se establecen multas y cárcel como sanciones por la violación de la ley.

REALIDAD: El que cometa actos delictivos en violación de una ley se arriesga a ser sancionado. El DHHS dará todas las oportunidades de cumplir con la ley y llevará a cabo todas las orientaciones necesarias antes de proceder a imponer las sanciones.

MITO: El Departamento de Salud Federal y/o Medicare certifican personas, programas de computadoras y/o sistemas como especialialistas o como que logran el cumplimiento con HIPAA.

HIPAA: Falso, ni Medicare ni el Departamento de Salud Federal certifican personas, ni programas, ni sistemas como especialistas que logran cumplimiento con HIPAA

MITO: No se pueden llamar los pacientes por nombre.

HIPAA: Falso, se puede seguir llamando pacientes por su nombre. (Ver situaciones discutidas en el Federal Register).

REALIDAD: Esta medida númerica es práctica para algunos escenarios, pero no es requerida**.**

MITO: Los expedientes no se pueden guardar por número de seguro social o por orden alfabético.

HIPAA: Sólo se requiere asegurar la confidencialidad de los récords.

REALIDAD: Falso, quisiéramos saber de dónde sale ésta premisa.