

CONFIDENCIALIDAD (HIPAA)

INTRODUCCION

Este capítulo intenta dar una explicación breve de la Ley de Confidencialidad HIPAA, la cual es una ley federal que se estableció para ayudar a proteger su derecho a la confidencialidad y seguridad respecto a la transmisión de su información de salud.

¿Qué es la HIPAA?

Las Normas para la Confidencialidad de la Información de Salud del Individuo (la Regla de Confidencialidad) fueron establecidas como parte de la Ley de Responsabilidad y Portabilidad del Seguro Médico de 1996 (HIPAA) De acuerdo con la Regla de Confidencialidad, todos los proveedores de atención de salud y los planes de salud son considerados “entidades regidas” y están obligados a proteger su información por medio del cumplimiento con la Regla de Confidencialidad. Estas “entidades regidas” y sus suministradores o “asociados” (definido a continuación) con quien comparten información de salud tienen la obligación de preparar y establecer métodos específicos, procesos y formas con el propósito de salvaguardar su información de salud.⁽³⁾

Al ir leyendo este capítulo verá palabras en comillas; esas palabras son términos comúnmente usados en la Regla de Confidencialidad y requieren atención especial.

¿Qué es entidad regida?

“Entidad regida” es cualquier entidad que está obligada por ley a cumplir con la Regla de Confidencialidad. En general, entre las entidades regidas se encuentran: (1) los proveedores de atención de salud; y (2) los planes de salud que transmiten información de salud en forma electrónica.⁽⁴⁾

Proveedor de atención de salud

“Proveedor de atención de salud” es el proveedor de servicios médicos o de salud y cualquier otra persona u organización que suministra, factura o recibe pago por la

(3) Algunos ejemplos de “información de salud protegida” son: el nombre de la persona, así como todo dato de identificación del individuo, tal como su número telefónico, historial de salud, diagnósticos, historial de reclamaciones, domicilio y número de Seguro Social.

(4) Al igual que los proveedores de atención de salud y los planes de salud, los “bancos de información de salud” también son entidades regidas. El término “bancos de información de salud” incluye a las agencias de facturación, las compañías de reproceso de precios y los sistemas comunitarios de información de salud que procesan o ayudan a procesar información de salud.

atención de salud en el curso normal de negocio. Entre algunos ejemplos de proveedores de atención de salud encuentran los doctores, hospitales, agencias de cuidado de salud en el hogar y los proveedores de materiales médicos durables.

Plan de salud

“Plan de salud” incluye a los planes de salud de grupo, aseguradoras que expiden seguros de salud, organizaciones de mantenimiento de salud, planes de prestaciones de empleado y cualquier otro plan individual o de grupo que provee o paga por el costo de atención médica. Esta categoría incluye virtualmente a todos los planes de salud de grupo, a los HMOs y a los programas gubernamentales para la atención de la salud (Medicare, CHAMPUS, etc.)

¿Quién es un asociado?

“Asociado” es cualquier persona o entidad que hace arreglos, desempeña o ayuda a una entidad regida a llevar a cabo una actividad en la que se usa o revela información médica considerada confidencial. Estas actividades incluyen el proceso de las reclamaciones, las gestiones de las reclamaciones, los análisis de datos, la revisión de utilización, el aseguramiento de calidad, el manejo de los beneficios, así como cualquier otra actividad similar regida por la Regla de Confidencialidad.

Entre algunos ejemplos de “asociado” se encuentran las personas que proveen servicios de proceso de reclamaciones, servicios jurídicos, complementación de datos, servicios actuariales u otros servicios que usan información de salud protegida.

¿Por qué es importante la diferencia entre entidad regida y asociado?

Las entidades regidas están automáticamente obligadas a cumplir con la Regla de Confidencialidad HIPAA. Las entidades regidas están obligadas por HIPAA a firmar acuerdos con sus asociados, acuerdos que obligan a sus asociados a conducirse según dicta la Regla de Confidencialidad con el objeto de resguardar información protegida. Los asociados quedan sujetos a cumplir con los preceptos de HIPAA solo cuando el acuerdo ha sido firmado y entra en vigor.

¿Qué es la información de salud protegida?

“Información de salud protegida” (o “PHI” según siglas en inglés) es básicamente los datos identificadores en la información de salud que ya sea identifican al individuo o paciente directamente o permiten que indirectamente alguien identifique al individuo o paciente.

Entre los ejemplos de PHI se encuentran su nombre, domicilio, número de seguro social, historial de salud, historial de reclamaciones, información de consultas con doctor y la información sobre su padecimiento médico.

¿Qué es la Regla de Confidencialidad?

La Regla de Confidencialidad es un reglamento con el que las entidades regidas y sus asociados tienen que cumplir para resguardar y proteger su PHI. La Regla en general estipula que la entidad regida y sus asociados no pueden usar o revelar PHI, excepto cuando la ley lo permite.

¿Cuándo se puede usar o revelar mi PHI?

Tratamiento, pago o ejercicio del cuidado de salud

La Ley de Confidencialidad permite que la PHI se use o revele bajo ciertas circunstancias. Por ejemplo: su propia PHI puede serle revelada a usted. También, su PHI puede ser revelada a otros según dispuesto en un consentimiento por escrito firmado por usted.

La Regla de Confidencialidad permite que las entidades regidas revelen la PHI para los siguientes propósitos: (1) “tratamiento”, (2) “pago”, o (3) “ejercicio de atención de salud”.

Excepción para miembros de familia

Existen ciertas circunstancias en las que la PHI, sin que usted haya dado consentimiento por escrito, puede ser revelada a los miembros de su familia u otras personas, siempre y cuando usted tenga el derecho a aceptar u objetar antes que su PHI sea revelada.

Excepciones para salud pública

La Regla de Confidencialidad también enumera varias circunstancias, pertinentes a la salud pública o a procedimientos legales/gubernamentales en las que se puede usar o revelar su PHI sin que usted haya dado consentimiento u autorización y sin darle una oportunidad para aceptar u objetar. La mayoría de estas circunstancias aplicarán a los entornos clínicos. ⁽⁵⁾

(5) Una entidad regida puede, hasta cierto grado, revelar PHI: (1) si la ley lo requiere; (2) para actividades de salubridad pública; (3) para reportar maltrato, abandono o violencia doméstica; (4) para actividades de supervisión de salud; (5) para procedimientos judiciales y administrativos; (6) para propósitos de imponer el cumplimiento a las leyes; (7) para donación de órganos, tejidos u ojos de cadáver; (8) para propósitos de investigaciones clínicas; (9) para evitar amenaza seria a la salud o seguridad; y (10) para funciones gubernamentales especializadas. Cada una de estas categorías tiene definiciones específicas de actividades que caen dentro de la categoría, y cada una tiene límites respecto a la información que se puede revelar.

Excepción para revelar información sin datos identificadores

Las entidades regidas también pueden revelar información de la que han extraído todo dato identificador (esa información a la cual todas las características identificadoras se le han eliminado) de acuerdo a la Regla de Confidencialidad, la cual dispone estipulaciones específicas respecto a la extracción de datos identificadores PHI. Los datos que podrían extraer de su PHI para revelación de información sin datos identificadores son: su nombre; subdivisión geográfica si menor que un estado; incluso su domicilio, condado y código postal; todos los elementos de fechas, incluso su fecha de nacimiento, fechas de admisión, etc.; números telefónicos y direcciones; número de seguro social; números de sus expedientes médicos; números de sus cuentas; números de beneficiarios del plan de salud; identificadores de vehículo, aparatos o biométricos; imágenes fotográficas u otras imágenes; o cualquier otra característica especial de identificación. Cuando al grado en el que a la información de salud se le ha extraído todo dato identificador de acuerdo a la Regla de Confidencialidad, la información ya no es PHI y ya no está sujeta a los reglamentos.

Revelaciones y usos incidentales

El uso o revelación incidental de su PHI está permitido en el punto que ocurre como derivado de un uso o revelación que de otro modo está permitido bajo la Ley de Confidencialidad. El uso o revelación incidental está permitido únicamente en el punto que la entidad regida aplica salvaguardas razonables de acuerdo a los estándares mínimos necesarios explicados a continuación.

¿Qué es el “estándar mínimo” necesario?

Como regla general, cuando una entidad regida o asociado usa o revela su PHI, el estándar “mínimo necesario” aplica. Esto significa que se deben hacer esfuerzos razonables para limitar la revelación de su PHI al mínimo de información necesaria para lograr el objetivo del propósito del uso o revelación.

¿Qué es el aviso y cuando se usa?

La Regla de Confidencialidad requiere que las entidades regidas le den aviso respecto a los derechos que la Regla de Confidencialidad le confiere, y de los usos o revelaciones potenciales de su PHI. La Regla de Confidencialidad contiene información específica para el formato del aviso y la información que debe contener el aviso, incluso: (1) declaración específica comunicándole el propósito del aviso; (2) descripción de cuando menos un ejemplo de los tipos de usos o revelaciones que la entidad regida podría hacer respecto a los propósitos respecto a tratamiento, pago o ejercicio del cuidado de salud; (3) una descripción de los otros propósitos para los cuales la

entidad regida podría estar permitida u obligada a usar o revelar PHI sin su autorización; y (4) declaraciones separadas que son obligatorias si la entidad regida está involucrada en ciertas actividades listadas en la Regla de Confidencialidad.⁽⁶⁾

¿Qué es la forma de autorización y cuándo se usa?

La autorización permite a la entidad regida o asociado usar o revelar su PHI a una persona particular o a una entidad para un propósito específico. Un ejemplo de cuando una autorización podría ser firmada por el paciente es cuando la revelación del PHI es para propósitos de mercadeo. En general, la autorización permite, si usted decide firmarla, la revelación de su PHI a una entidad no regida o a uno que no es asociado.⁽⁷⁾

¿Cuáles son las mayores diferencias entre el aviso y la autorización?

El aviso es un documento que le informa sobre como la entidad regida utilizará o revelará el PHI suyo y cuales pasos la entidad regida tomará para proteger su PHI. La autorización es una forma que usted decide si firmar o no, en la cual autoriza a una entidad regida a usar o revelar su PHI para propósitos aparte de tratamiento, pago o ejercicio de cuidado de salud.

¿Cuáles son sus derechos respecto a su PHI?

La Regla de Confidencialidad le otorga el derecho a tener acceso a su PHI, el derecho a que se le hagan correcciones a su PHI y el derecho a que le den cuentas/justificación de las revelaciones de su PHI. Estos derechos se los deben explicar en la forma de aviso.

- (6) Estas actividades incluyen, por ejemplo: la comunicación con el individuo para recordatorios de citas, el envío de información de tratamientos alternativos y otros beneficios o servicios relativos a la salud, y actividades para recabar fondos.
- (7) La Regla de Confidencialidad requiere que la autorización: (1) describa, de una manera específica y significativa la información que se va a usar o revelar; (2) el nombre o de otra manera específicamente identifique a la persona o clase de personas a quien se le va a hacer la revelación; (3) contenga una fecha de vencimiento o un evento de vencimiento relativo a usted o el propósito de la revelación; (4) contenga declaraciones respecto al derecho suyo para revocar la autorización, y una descripción de cómo revocar la autorización; (5) contenga una declaración informándole que la información a revelar podría estar sujeta a que el destinatario la revele o podría no estar protegida por la autorización una vez que esté en manos del destinatario; y (6) tenga su firma y esté fechada.

¿Cuándo entró en vigor la Regla de Confidencialidad?

La Regla de Confidencialidad está actualmente en vigor. En general, las entidades regidas tienen que haber estado en cumplimiento para el 14 de abril del 2003. Aunque los planes pequeños de salud (los planes de salud con recibos anuales de \$5 millones, o menos) tuvieron hasta el 14 de abril del 2004 para entrar en cumplimiento.

¿Qué pasa si una entidad regida o asociado infracciona la Regla de Confidencialidad?

El Departamento de Salud y Servicios Humanos puede llevar a cabo una inspección de cumplimiento de cualquier entidad regida para determinar si la entidad está cumpliendo con la Regla de Confidencialidad.

¿Cómo interacciona la HIPAA con las leyes estatales?

La Regla de Confidencialidad es una ley federal. En general, si hay conflicto entre la ley federal y la ley estatal, la ley federal es la que aplica. Pero, la Regla de Confidencialidad también requiere que si las leyes de un estado en particular discrepan con la Regla de Confidencialidad y la ley del estado es más rigurosa (proporciona más protección) la ley estatal o la porción de la ley estatal que es más rigurosa sea la que rija en lugar de la Regla de Confidencialidad.