VITRA Health

Educación para Cuidadores - Edición de octubre

HIPAA y Privacidad

Resumen del Reglamento de Seguridad de HIPAA

Este es un resumen de los elementos clave del Reglamento de Seguridad, el cual incluye quiénes tienen cobertura, qué información está protegida y qué medidas de seguridad deben implementarse para garantizar la protección adecuada de la información médica protegida electrónica. Debido a que se trata de una descripción general del Reglamento de Seguridad, no se abordan todos los detalles de cada disposición.

Introducción

La Ley de Portabilidad y Responsabilidad de los Seguros de Salud (*Health Insurance Portability and Accountability Act*, o HIPAA, por sus siglas en inglés) de 1996 exigió al Secretario del Departamento de Salud y Servicios Humanos de EE.UU. (*U.S. Department of Health and Human Services*, o HHS, por sus siglas en inglés) que desarrollara regulaciones que protegieran la privacidad y seguridad de cierta información relacionada con la salud.

Para cumplir con este requisito, el HHS publicó lo que comúnmente se conoce como el Reglamento de Privacidad de HIPAA (*HIPAA Privacy Rule*) y el Reglamento de Seguridad de HIPAA (*HIPAA Security Rule*). El Reglamento de Privacidad, o los Estándares para la Privacidad de la Información de Salud Individualmente Identificable (*Standards for Privacy of Individually Identifiable Health Information)*, establece estándares a nivel nacional para la protección de cierta información relacionada con la salud. Los Estándares de Seguridad para la Protección de la Información Médica Protegida Electrónica (*Security Standards for the Protection of Electronic Protected Health*), es decir, el Reglamento de Seguridad, establece un conjunto de normas de seguridad a nivel nacional para proteger cierta información médica que se conserve o transfiera de manera electrónica. El Reglamento de Seguridad hace operativas las protecciones contenidas en el Reglamento de Privacidad al abordar las medidas de seguridad técnicas y no técnicas que las organizaciones llamadas “entidades cubiertas” deben implementar para proteger la “información de salud electrónica protegida” (e-PHI) de las personas. Dentro del HHS, la Oficina de Derechos Civiles (*Office for Civil Rights*, u OCR, por sus siglas en inglés) tiene la responsabilidad de hacer cumplir los Reglamentos de Privacidad y de Seguridad con actividades de cumplimiento voluntario y multas monetarias civiles.

Antes de HIPAA, no existía en la industria del cuidado de la salud ningún conjunto de estándares de seguridad ni requisitos generalmente aceptados para proteger la información relacionada con la salud. Al mismo tiempo, las nuevas tecnologías estaban evolucionando y la industria del cuidado de la salud comenzó a alejarse de los procesos en papel y a confiar más en el uso de sistemas de información electrónicos para pagar coberturas de seguro, responder

preguntas de cumplimiento de requisitos, proporcionar información relacionada con la salud y realizar una amplia gama de funciones administrativas y clínicas.

Hoy en día, los proveedores utilizan aplicaciones clínicas como sistemas computarizados de ingreso de órdenes médicas (CPOE), registros de salud electrónicos (EHR) y sistemas de radiología, farmacia y laboratorio. Los planes de salud brindan acceso a los pagos de coberturas de seguro y a las consultas de atención médica, así como aplicaciones de autoservicio para los miembros. Si bien esto significa que la fuerza laboral médica puede tener más movilidad y ser más eficiente (ya que los médicos pueden revisar los expedientes de los pacientes y verificar los resultados de las pruebas desde cualquier lugar), el aumento en la tasa de adopción de estas tecnologías aumenta los riesgos potenciales de seguridad.

Un objetivo principal del Reglamento de Seguridad es proteger la privacidad de la información de las personas relacionada con la salud y, al mismo tiempo, permitir que las entidades cubiertas adopten nuevas tecnologías para mejorar la calidad y la eficiencia de la atención al paciente. Dado que el mercado de atención médica es muy diverso, el Reglamento de Seguridad está diseñado para ser flexible y escalable, de modo que una entidad cubierta pueda implementar políticas, procedimientos y tecnologías que sean apropiados para el tamaño particular de esa entidad, su estructura organizativa y los riesgos que corre la e-PHI de sus consumidores.

Este es un resumen de los elementos clave del Reglamento de Seguridad y no pretende ser una guía completa ni exhaustiva para el cumplimiento. Las entidades reguladas por los Reglamentos de Privacidad y Seguridad están obligadas a cumplir con todos sus requisitos aplicables y no deben confiar en este resumen como fuente de información ni como asesoramiento legal. Para facilitar la revisión de los requisitos completos del Reglamento de Seguridad, las disposiciones del Reglamento a las cuales se hace referencia en este resumen se citan en las notas finales. Visite nuestra sección del Reglamento de Seguridad para ver la normativa completa y obtener información útil adicional sobre cómo se aplica la misma. En caso de existir algún conflicto entre este resumen y el Reglamento, siempre prevalecerá el Reglamento.

Antecedentes reglamentarios legales

Las disposiciones de la Simplificación Administrativa de la Ley de Portabilidad y Responsabilidad del Seguro Médico de 1996 (HIPAA, Título II) exigieron que el Secretario del HHS publicara estándares nacionales para la seguridad de la información médica protegida electrónica (e-PHI), el intercambio electrónico y la privacidad y seguridad de la información relacionada con la salud.

HIPAA solicitó al Secretario del HHS que emitiera normas de seguridad con respecto a las medidas para proteger la confidencialidad, integridad y disponibilidad de la e-PHI que conservan o transmiten las entidades cubiertas. El HHS desarrolló una normativa propuesta y la publicó para comentarios públicos el 12 de agosto de 1998. El HHS recibió aproximadamente

2,350 comentarios públicos. La normativa final, que es el Reglamento de Seguridad, se publicó el 20 de febrero de 2003.[2] El Reglamento especifica una serie de procedimientos de seguridad administrativa, técnica y física que las entidades cubiertas deben seguir para asegurar la confidencialidad, integridad y disponibilidad de la e-PHI. El texto de la normativa final se puede encontrar en el 45 CFR Parte 160 y Parte 164, Subpartes A y C.

¿Quiénes están cubiertos por el Reglamento de Seguridad?

El Reglamento de Seguridad se aplica a los planes de salud, a las cámaras de compensación de atención médica y a cualquier proveedor de atención médica que transmita información médica en formato electrónico en relación con una transacción para la cual el Secretario del HHS ha adoptado normas conforme a HIPAA (las "entidades cubiertas") y a sus socios comerciales. Si necesita ayuda para determinar su cobertura, use la herramienta de decisión del CMS. Conozca más detalles acerca de las entidades cubiertas en el Resumen del Reglamento de Privacidad de HIPAA.

Socios comerciales

La Ley HITECH de 2009 amplió las responsabilidades de los socios comerciales bajo el Reglamento de Seguridad de HIPAA. El HHS desarrolló normativas para implementar y aclarar estos cambios. Consulte los lineamientos adicionales sobre los socios comerciales.

¿Qué información está protegida?

La Información de Salud Protegida Electrónica. El Reglamento de Privacidad de HIPM protege la privacidad de la información de salud identificable individualmente, llamada Información de Salud Protegida (PHI, por sus siglas en inglés), tal como se explica en el Reglamento de Privacidad. El Reglamento de Seguridad protege un subconjunto de información cubierta por el Reglamento de Privacidad, que es toda la información de salud identificable individualmente que una entidad cubierta crea, recibe, mantiene o transmite en forma electrónica. El Reglamento de Seguridad denomina a esta información "información de salud electrónica protegida" (e-PHI). El Reglamento de Seguridad no se aplica a la PHI transmitida oralmente o por escrito.

Reglas generales:

El Reglamento de Seguridad exige que las entidades cubiertas mantengan medidas de seguridad administrativas, técnicas y físicas razonables y apropiadas para proteger la e-PHI. Específicamente, las entidades cubiertas deben:

- Asegurar la confidencialidad, integridad y disponibilidad de toda la e-PHI que creen, reciban, mantengan o transmitan.

- Identificar y proteger contra amenazas razonablemente anticipadas a la seguridad o integridad de la información.
- Proteger contra usos o divulgaciones razonablemente previstos o no permisibles.
- Velar por el cumplimiento por parte de su personal.

El Reglamento de Seguridad define “confidencialidad” en el sentido de que la e-PHI no esté disponible ni sea revelada a personas que no estén debidamente autorizadas. Los requisitos de confidencialidad del Reglamento de Seguridad respaldan las prohibiciones del Reglamento de Privacidad contra divulgaciones y usos indebidos de la PHI. El Reglamento de Seguridad también promueve los dos objetivos adicionales de mantener la integridad y la disponibilidad de la e-PHI. Según el Reglamento de Seguridad, “integridad” significa que la e-PHI no se altere ni se destruya de manera no autorizada. Por último, “disponibilidad” significa que la e-PHI esté accesible y sea utilizable cuando una persona debidamente autorizada la solicite.

El HHS reconoce que las entidades cubiertas van desde el proveedor más pequeño hasta el plan de salud más grande que funciona en varios estados. Por lo tanto, el Reglamento de Seguridad es flexible y escalable para permitir que las entidades cubiertas analicen sus propias necesidades e implementen soluciones adecuadas para sus entornos específicos. Lo que sea apropiado para una entidad cubierta en particular dependerá de la naturaleza del negocio de la entidad cubierta, así como del tamaño y los recursos de la entidad cubierta.

Por lo tanto, cuando una entidad cubierta esté decidiendo qué medidas de seguridad implementar, el Reglamento no dicta esas medidas, sino que exige que la entidad cubierta considere:

- Su tamaño, su complejidad y sus capacidades.
- Su infraestructura técnica, de hardware y de software.
- El costo de las medidas de seguridad.
- La probabilidad y el posible impacto de los riesgos potenciales para la e-PHl.

Las entidades cubiertas deben revisar y modificar sus medidas de seguridad para continuar protegiendo la e-PHI en un entorno cambiante.

Análisis y gestión de riesgos

Las disposiciones de las Garantías Administrativas del Reglamento de Seguridad exigen que las entidades cubiertas lleven a cabo un análisis de riesgo como parte de sus procesos de gestión de la seguridad. Las disposiciones de análisis y gestión de riesgos del Reglamento de Seguridad se abordan aquí por separado, ya que al ayudar a determinar qué medidas de seguridad son razonables y apropiadas para una entidad cubierta en particular, el análisis de riesgos afecta la implementación de todas las garantías contenidas en el Reglamento de Seguridad.

Un proceso de análisis de riesgos incluye, pero no se limita a, las siguientes actividades:

- Evaluar la probabilidad y el impacto de los riesgos potenciales para la e-PHI.
- Implementar medidas de seguridad adecuadas para abordar los riesgos identificados en el análisis de riesgos.
- Documentar las medidas de seguridad seleccionadas y, en su caso, la justificación de la adopción de dichas medidas.
- Mantener protecciones de seguridad continuas, razonables y apropiadas.

El análisis de riesgos debe ser un proceso continuo, a través del cual la entidad cubierta revise periódicamente sus registros para rastrear el acceso a la PHI y detectar incidentes de seguridad,[12] evaluar periódicamente la efectividad de las medidas de seguridad implementadas,[13] y reevaluar periódicamente los riesgos potenciales para la e-PHI.

Medidas preventivas de administración

- **Proceso de gestión de la seguridad:** Como se explicó en la sección anterior, la entidad cubierta debe identificar y analizar los riesgos potenciales para la e-PHI, y debe implementar medidas de seguridad que reduzcan los riesgos y vulnerabilidades a un nivel razonable y apropiado.
- **Personal de seguridad:** La entidad cubierta debe designar a un oficial de seguridad como la persona responsable de desarrollar e implementar sus políticas y procedimientos de seguridad.
- **Gestión del acceso a la información:** De acuerdo con el estándar del Reglamento de Privacidad que limita los usos y las divulgaciones de la PHI al "mínimo necesario", el Reglamento de Seguridad exige que la entidad cubierta implemente políticas y procedimientos para autorizar el acceso a la PHI solamente cuando dicho acceso sea apropiado en función del rol del usuario o destinatario (control de acceso según el rol).
- **Capacitación y gestión de la fuerza laboral:** La entidad cubierta debe proporcionar la autorización y supervisión adecuadas de los miembros del personal que trabajan con la e-PHI.[17] La entidad cubierta debe capacitar a todos los miembros del personal con respecto a sus políticas y procedimientos de seguridad,[18] y debe tener y aplicar sanciones apropiadas a los miembros del personal que infrinjan su políticas y procedimientos.
- **Evaluación:** La entidad cubierta debe realizar una evaluación periódica de qué tan bien sus políticas y procedimientos de seguridad cumplen con los requisitos del Reglamento de Seguridad.

Medidas preventivas físicas

- **Acceso y control de las instalaciones**: La entidad cubierta debe limitar el acceso físico a sus instalaciones, garantizando a la vez que se permita el acceso autorizado.

- **Seguridad de las estaciones de trabajo y los dispositivos:** La entidad cubierta debe implementar políticas y procedimientos para especificar el uso adecuado y el acceso a las estaciones de trabajo y los medios electrónicos.[22] La entidad cubierta también debe tener políticas y procedimientos establecidos con respecto a la transferencia, eliminación, disposición y reutilización de los medios electrónicos para garantizar una protección adecuada de la información médica protegida electrónica (e-PHI).

Medidas preventivas técnicas:

- **Control de acceso:** La entidad cubierta debe implementar políticas y procedimientos técnicos que permitan que solamente las personas debidamente autorizadas tengan acceso a la información médica protegida electrónica (e-PHI).
- **Controles de auditoría:** La entidad cubierta debe implementar hardware, software y/o mecanismos de procedimiento para almacenar y examinar el acceso y otras actividades en los sistemas de información que contienen o usan e-PHI.
- **Controles de integridad:** La entidad cubierta debe implementar políticas y procedimientos para garantizar que la e-PHI no se altere ni se destruya indebidamente. Se deben implementar medidas electrónicas para confirmar que la e-PHI no haya sido alterada o destruida de manera inapropiada.
- **Seguridad de transmisión:** La entidad cubierta debe implementar medidas técnicas de seguridad que protejan contra el acceso no autorizado a la PHI que se transmite a través de una red electrónica.

Requisitos organizativos

- **Responsabilidades de la entidad cubierta:** Si la entidad cubierta tiene conocimiento de una actividad o práctica del socio comercial que constituya un incumplimiento material o una infracción de la obligación del asociado comercial, la entidad cubierta debe tomar medidas razonables para subsanar el incumplimiento o poner fin a dicha infracción. Las infracciones incluyen la falta de implementación de medidas preventivas que protejan razonable y adecuadamente la e-PHI.
- **Contratos con los socios comerciales:** El HHS desarrolló normativas relacionadas con las obligaciones de los socios comerciales y los contratos con los socios comerciales, en virtud de la Ley HITECH de 2009.

Políticas y procedimientos y requisitos de documentación

- Las entidades cubiertas están obligadas a cumplir con todos los “estándares” del Reglamento de Seguridad. Sin embargo, el Reglamento de Seguridad clasifica ciertas especificaciones de implementación dentro de esos estándares como “abordables”, mientras que otras especificaciones se clasifican como “requeridas”. Por un lado, se deben llevar a cabo las especificaciones de implementación “requeridas”. Por otro lado, la

designación de “abordable” no significa que una especificación de implementación sea opcional. Sin embargo, permite que las entidades cubiertas determinen si la especificación de implementación abordable es razonable y apropiada para esa entidad cubierta. Si no lo es, el Reglamento de Seguridad permite que la entidad cubierta adopte una medida alternativa que logre el propósito de la normativa si dicha medida alternativa es razonable y apropiada.

- Actualizaciones. La entidad cubierta debe revisar y actualizar periódicamente su documentación en respuesta a los cambios ambientales u organizacionales que afecten la seguridad de la información de salud protegida electrónica (e-PHI).

Leyes estatales

- Derecho preferente de compra. En general, las leyes estatales que son contrarias a las reglamentaciones de la HIPAA quedan anuladas por los requisitos federales, lo cual significa que se aplicarán los requisitos federales.[32] “Contraria” significa que sería imposible para una entidad cubierta cumplir tanto con los requisitos estatales como federales, o que la disposición de la ley estatal representa un obstáculo para lograr todos los propósitos y objetivos de las disposiciones de simplificación administrativa de HIPAA.

Ejecución y sanciones por incumplimiento

- Cumplimiento: El Reglamento de Seguridad establece un conjunto de estándares a nivel nacional en cuanto a la confidencialidad, integridad y disponibilidad de la e-PHI. La Oficina de Derechos Civiles (OCR, por sus siglas en inglés) del Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés) es el ente responsable de administrar y hacer cumplir estos estándares, de acuerdo con su aplicación del Reglamento de Privacidad, y puede realizar investigaciones de quejas y revisiones de cumplimiento.

Fechas de cumplimiento:

- Cronograma de cumplimiento: Todas las entidades cubiertas, excepto los “planes de salud pequeños”, debían haber cumplido con el Reglamento de Seguridad a más tardar el 20 de abril de 2005. Los planes de salud pequeños tuvieron un plazo hasta el 20 de abril de 2006 para cumplir con el Reglamento de Seguridad.

Copias de los Reglamentos y materiales afines

- Consulte nuestra sección Texto Combinado de las Normativas de todos los Reglamentos (*Combined Regulation Text of All Rules)* de nuestro sitio, para conocer el conjunto completo de Reglamentos de Simplificación Administrativa de HIPAA, así como HIPAA para Profesionales, para obtener material de orientación adicional.

Fuente: www.hhs.gov