LA REGLA DE SEGURIDAD DE HIPAA
PREGUNTAS MÁS FRECUENTES

1- ¿Es obligatorio el cifrado en la Regla de Seguridad de HIPAA?

No. La regla de seguridad final hizo el uso de cifrado una especificación de implementación factible. Ver 45 CFR §§ 164.312(a)(2)(iv) y 164.312(e)(2)(ii). Las entidades cubiertas usan portales como el Internet y el sistema de correo electrónico de formas diferentes, y ningún tipo de solución de ínter operador sencillo cifrado para comunicarse con otros portales existe. Fijar un solo cifrado estándar habría podido colocar una carga injusta financiera y técnica en algunas de las entidades cubiertas.

La especificación de la implementación del cifrado es factible, y debe por lo tanto ser implementada si, después de una evaluación, la entidad ha determinado que la especificación es una seguridad razonable y apropiada en su ambiente. Si la entidad decide que la especificación direccionable implementada no es razonable y apropiada, debe documentar esa determinación e implementar una medida alterna equivalente, presumiendo que la alternativa es razonable y apropiada, o si el estándar puede ser resuelto de otra manera, la entidad cubierta puede elegir no implementar la especificación implementada o ninguna medida alterna equivalente.

2- ¿Qué es cifrado?

El cifrado es un método de convertir un mensaje original del texto regular en texto codificado. El texto es cifrado por medio de un algoritmo (tipo de fórmula). Sí la información es cifrada, habría una escasa probabilidad de que cualquier persona, exceptuando la parte recibidora que tiene la llave al código o al acceso a otro proceso confidencial, podría descifrar (traducir) el texto y convertirlo en un texto sencillo, comprensible.

3- ¿ La Regla de Seguridad permite enviar información de salud protegida (PHI, por sus siglas en inglés) electrónicamente por correo electrónico o el Internet? ¿Si es así, qué protecciones deben ser aplicadas?

La Regla de Seguridad no prohíbe explícitamente el uso de correo electrónico para enviar PHI electrónico. Sin embargo, los estándares para el control de acceso, (el § de 45 CFR 164.312(a)) la integridad (§ de 45 CFR 164.312(c)(1)), y la seguridad de la transmisión (§ de 45 CFR 164.312(e)(1)) requieren de las entidades cubiertas implementar políticas y procedimientos para restringir el acceso a, proteger la integridad de, y proteger en contra del acceso no autorizado al PHI electrónico. El estándar para la seguridad de la transmisión (§ 164.312(e)) también incluye las especificaciones factibles para los controles de integridad y cifrado. Esto significa que la entidad cubierta debe determinar su uso de portales abiertos, identificar los medios disponibles y apropiados para proteger el PHI electrónico según se transmite, seleccionar una solución, y documentar la decisión. La Regla de Seguridad permite que el PHI electrónico sea enviado sobre un portal abierto electrónico mientras se proteja adecuadamente.

4- ¿ Los requisitos de la Regla de Seguridad para el control de acceso, tal como término de sesión automático, se aplican a los empleados que trabajan de su casa o tienen la base de su oficina en el hogar y si el empleado tiene acceso a PHI electrónico?

Sí. Las entidades cubiertas que permiten a empleados desplazarse por vía telefónica o trabajar desde oficinas con base en el hogar y tienen acceso al PHI electrónico, deben implementar una seguridad apropiada para proteger los datos de la organización. La especificación de implementación automática del término de sesión es direccionable, y debe por lo tanto ser implementada si, después de una evaluación, la entidad ha determinado que la especificación es una razonable y de seguridad apropiada en su ambiente. Si la entidad decide que la especificación de la implementación puesta en práctica del término de sesión no es razonable y no es apropiada, debe documentar esa determinación e implementar una medida alterna equivalente, presumiendo que la alternativa es razonable y apropiada, o si el estándar puede ser resuelto de otra manera, la entidad cubierta puede elegir no implementar la especificación de la implementación o cualquier medida alterna equivalente.
La gerencia del acceso de información y los estándares del control de acceso, sin embargo, requieren que la entidad cubierta implemente políticas y procedimientos para autorizar el acceso a PHI electrónico y a las políticas y a los procedimientos técnicos para permitir el acceso solamente a esas personas o programas de computadora a los que se le han concedido apropiadamente los derechos de acceso.

5- ¿ Cuál es la diferencia entre el Análisis de Riesgo y Gerencia de Riesgo en la Regla de Seguridad de HIPAA?

El análisis de riesgo es la evaluación de los riesgos y vulnerabilidad que podrían impactar negativamente la confidencialidad, la integridad, y la disponibilidad del PHI electrónico retenido por una entidad cubierta, y de la probabilidad de la ocurrencia.

El análisis del riesgo puede incluir inventario de todos los sistemas y usos que se utilicen para tener acceso y los datos de la casa, y clasificarlos por el nivel del riesgo. Un análisis cuidadoso y exacto del riesgo consideraría todas las pérdidas relevantes que esperarían si las medidas de seguridad no estaban en lugar, incluyendo pérdida o el daño de datos, sistemas corruptos de datos, y ramificaciones anticipadas de tales pérdidas o daño.

La gerencia de riesgo es la implementación actual de las medidas de seguridad de reducir suficientemente un riesgo de las organizaciones de perder o de comprometer su PHI electrónico y de resolver los estándares generales de la seguridad.

6- ¿Qué es una vulnerabilidad del sistema?

Una vulnerabilidad del sistema es un defecto o una debilidad en un sistema, debido a su diseño, a la instalación, a la carencia de políticas y de procedimientos, o a algún otra causa. Cualesquiera de estas debilidades, ya sean intencionales o accidentales, podían potencialmente resultar en una abertura o un uso inapropiado o divulgación de PHI electrónico. Algunas vulnerabilidades pueden ser causadas por políticas ineficaces con respecto a usuario o entrar las identificaciones y las contraseñas, los agujeros o las debilidades en algunas de las herramientas de los programas de computadora, o los defectos en el sistema operativo, aplicación o acceso de control inadecuado.

7- ¿ Cómo sabemos si nuestra organización y nuestros sistemas están en cumplimiento con los requisitos de la Regla de Seguridad de HIPAA?

El propósito de la regla final es adoptar los estándares nacionales para la seguridad de proteger la confidencialidad, la integridad, y la disponibilidad de PHI electrónico que es recolectado, conservado, utilizado o transmitido por una entidad cubierta. El cumplimiento es diferente para cada organización y ninguna estrategia servirá a todas las entidades cubiertas. El cumplimiento no es una meta de una sola vez, debe ser sostenido. El cumplir con el estándar de evaluación en el § 164.308(a)(8) permitirá que las entidades cubiertas conserven el cumplimiento. Realizando una evaluación técnica y no técnica periódica una entidad cubierta podrá dirigir la implementación de los estándares y los cambios ambientales u operacionales futuros que afectan la seguridad de PHI electrónico.

Las entidades cubiertas deben mirar al § 164,306 de la Regla de Seguridad para dirección que apoye las decisiones sobre cómo cumplir con los estándares y las especificaciones de implementación contenidas en el §§ 164,308, 164,310, 164,312, 164,314, y 164,316. En general, esto incluye la ejecución de un análisis de riesgo; implementando medidas de seguridad razonables y apropiadas; y documentando y manteniendo las políticas, procedimientos y otra documentación requerida.

8- ¿Nos requieren certificar nuestra organización con los estándares de seguridad?

No, no hay ningún estándar o especificación de implementación que requiera a una entidad cubierta certificar el cumplimiento. El estándar de evaluación 164.308(a)(8) requiere a las entidades cubiertas realizar una evaluación técnica y no técnica periódica que establezca el grado al cual las políticas de seguridad de la entidad y los procedimientos cumplen con los requisitos de seguridad.

La evaluación se puede realizar internamente por la entidad cubierta. También hay organizaciones externas que proveen evaluaciones o servicios de "certificaciones''. Una entidad cubierta puede tomar la decisión de negocio de tener una organización externa que realice estos tipos de servicios. Es importante observar que HHS no endosa ni reconoce de otra manera "certificaciones'' de organizaciones privadas y tales certificaciones no absuelven a las entidades cubiertas de sus obligaciones legales bajo la Regla de Seguridad. Por otra parte, el funcionamiento de una certificación por una organización externa no imposibilita a HHS posteriormente de encontrar una violación de la seguridad.

9- ¿La Regla de Seguridad aplica a las comunicaciones escritas y orales?

No. La Regla de Seguridad es específica a PHI electrónico. Debe ser observado sin embargo que PHI electrónico también incluye respuesta de voz por teléfono y el sistema de fax devuelto porque se utilizan como dispositivos de entrada y salida para las computadoras. PHI electrónico no incluye faxes de papel-a-papel o tele conferencias de video o los mensajes de grabadoras, porque la información intercambiada no existió en forma electrónica antes de la transmisión. En contraste, la Regla de Privacidad de HIPAA dirige todos los medios de PHI, incluyendo escrito y oral. La información sobre la Regla de Privacidad se puede encontrar en la línea: http://www.hhs.gov/ocr/hipaa/.

10- ¿Qué significa para la Regla de Seguridad de HIPAA la seguridad física?

Los salvaguarda físicos son medidas físicas, políticas, y procedimientos para proteger los sistemas de información electrónica de entidades cubiertas y edificios relacionados y el equipo de peligros naturales y ambientales, y la intrusión no autorizada. Los estándares bajo seguridad física incluyen facilidad de control de acceso, uso de la estación de trabajo, seguridad del sitio de trabajo, y dispositivo y control de los medios. La Regla de Seguridad requiere que las entidades cubiertas implementen los estándares físicos de seguridad para sus sistemas de información electrónica aun si tales sistemas están contenidos en las premisas de las entidades cubiertas o en otra localización.

10- ¿La Regla de Seguridad de HIPAA asigna los requisitos mínimos del sistema operativo para los sistemas de computadora personal usados por una entidad cubierta?

No. La Regla de Seguridad fue escrita para permitir flexibilidad para que las entidades cubiertas seleccionen la tecnología que mejor se ajuste a sus necesidades de organización. La Regla de Seguridad no especifica los requisitos mínimos para los sistemas operativos de la computadora personal, sino que asigna los requisitos por mandato para los sistemas de información con PHI electrónico. Por lo tanto, como parte del sistema de información, las capacidades de seguridad del sistema operativo pueden ser utilizada para cumplir con estándares de seguridad técnicos y especificaciones de implementación tales como controles de auditoria, identificación de usuario único, integridad, autentificación de la persona o de la entidad, o seguridad de la transmisión.

12- ¿La Regla de Seguridad de HIPAA requiere el uso de una firma electrónica o digital?

No, la Regla de Seguridad no requiere el uso de firmas electrónicas o digitales. Sin embargo, las firmas electrónicas o digitales se podrían utilizar como medida de seguridad si la entidad cubierta determina si el uso es razonable y apropiado.

Además, la regla final para adoptar un estándar de HIPAA para las firmas electrónicas todavía no se ha publicado. Consecuentemente, la implementación estándar de la firma electrónica no se requiere actualmente.

13- ¿Las entidades cubiertas requieren el uso de los documentos guías del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) referidas en el preámbulo final de la Regla de Seguridad?

No. Las entidades cubiertas pueden utilizar cualquiera de los documentos de NIST hasta el punto de proveer guías relevantes a las actividades de implementación de las organizaciones. Mientras que los documentos del NIST fueron mencionados en el preámbulo de la Regla de Seguridad, éste no los hace requeridos. De hecho, algunos de los documentos pueden no ser relevantes a las organizaciones pequeñas, ya que éstos estaban destinados a más grandes organizaciones gubernamentales.