HIPAA SERIE DE Seguridad

Temas de Seguridad

1 Seguridad 101 para Entidades Cubiertas

¿Qué es la Serie de Seguridad?

La serie de documentos de seguridad proporcionará una guía de parte de los Centros de Servicios de Medicare y Medicaid (CMS, por sus siglas en inglés) en la regla titulada "Los Estándares de Seguridad para la Protección de la Información Electrónica Protegida de la Salud", encontrado en 45 partes 160 y 164 de CFR, subparte A y la regla de C. Esta regla, conocida comúnmente como La Regla de Seguridad, fue adoptada para implementar provisiones en la Ley de Portabilidad y Contabilidad de Seguros de Salud de 1996 (HIPAA, por sus siglas en inglés). La serie contendrá ocho papeles, cada uno centrado en un asunto específico relacionado con la regla de Seguridad. Los documentos, que cubren los asuntos enumerados a la izquierda, se diseñaron para dar a las entidades cubiertas por HIPAA discernimiento sobre La Regla de Seguridad, y asistencia con la implementación de los estándares de seguridad. Mientras que no hay ningún acercamiento que garantiza una implementación con éxito en todos los estándares de seguridad, esta serie se dirige en explicar los requisitos específicos, el proceso difícil detrás de estos requisitos, y posibles formas de dirigir las provisiones. Este primer documento en la serie provee una descripción de La Regla de Seguridad y de su cruce con La Regla de Privacidad de HIPAA, las provisiones de la cual están en 45 partes 160 y 164 de CFR, el Subparte A y E.

Fechas Límites de Cumplimiento

No más tarde del 20 de abril de 2005 para todas las entidades cubiertas excepto planes pequeños de salud que tienen hasta no más tarde del 20 de abril de 2006.

Simplificación Administrativa

El congreso pasó la provisión de la Simplificación Administrativa de HIPAA, además de otras cosas, para proteger la privacidad y seguridad de cierta información de salud, y promover la eficiencia en la industria del cuidado de la salud mediante el uso de transacciones electrónicas estandarizadas. La industria del cuidado de la salud esta trabajando para cumplir el reto de estas metas mediante una implementación de éxito de la Simplificación Administrativa. El Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés) ha publicado unas reglas implementando un número de provisiones incluyendo:

Regulación de Seguridad

La Regla final de Seguridad se puede ver y descargar del sitio Web de CMS: http://www.cms.hhs.gov/hipaa/hipaa2

HIPAA Simplificación Administrativa

- Privacidad
- Transacciones Electrónicas y Serie de Código *
- Identificador Nacional
- Seguridad

*** NOTA:** La fecha limite original para el cumplimiento con las transacciones y los estándares de los códigos era el 16 de Octubre de 2002 para todas las entidades cubiertas excepto los planes pequeños de la salud, que tenían hasta el 16 de Octubre de 2003 para cumplir.

La ley de Cumplimiento de la Simplificación Administrativa proporcionó una extensión de un año a las entidades cubiertas que no eran planes pequeños de la salud, si los planes de cumplimiento eran sometidos a tiempo al HHS.

NOTA: La definición de las entidades cubiertas proporcionadas aquí resume las definiciones reales encontradas en las regulaciones. Para las definiciones de los tres tipos de entidades cubiertas, vea el 160,103 de 45 CFR el cual puede ser encontrado en:

www.hhs.gov/ocr/hipaa

- **Regla de Privacidad-** La fecha limite para el cumplimiento de los requisitos de privacidad que gobiernan el uso y divulgación de la información protegida de la salud (PHI) era el 14 de abril de 2003, a excepción de los planes pequeños que tenían hasta el 14 de abril de 2004 para la fecha limite. (La información protegida de la salud, o "PHI", se define en el 160,103 de 45 CFR, que aparece en el sitio Web de OCR en http://hhs.gov/ocr/hipaa.)

- **Las Transacciones Electrónicas y Regla de Códigos de Serie**- todas las entidades cubiertas deben haber estado en cumplimiento con los formatos estándares de las transacciones electrónicas y de los códigos de formatos de serie desde el 16 de octubre de 2003.

- **Los requisitos del identificador nacional para los patrones, los proveedores, y los planes de la salud** - el número de identificación de patrón (EIN, por sus siglas en inglés), publicado por el servicio de renta internas (IRS), fue seleccionado como el identificador para los patrones. Las entidades cubiertas deben utilizar este identificador efectivo el 30 de julio de 2004 (a excepción de los planes pequeños, que tienen hasta el 30 de julio de 2005). El identificador nacional del proveedor (NPI, por sus siglas en inglés) fue adoptado como el identificador único estándar de la salud para los proveedores del cuidado médico. La regla final es efectiva el 23 de mayo de 2005. Los proveedores pueden solicitar el NPI durante o después de esa fecha. La fecha del cumplimiento del NPI para todas las entidades cubiertas, excepto los planes pequeños de salud, el 23 de mayo de 2007; la fecha de cumplimiento para los planes pequeños de la salud es 23 de mayo de 2008. La regla del identificador del plan de salud se espera en los años que vienen.

- **La regla de seguridad**- todas las entidades cubiertas deben estar en cumplimiento con la regla de seguridad no más tarde del 20 de Abril de 2005, excepto los planes pequeños de la salud que deben cumplir no más tarde del 20 de abril de 2006. Las provisiones de la regla de seguridad aplican a la información de salud electrónica protegida (EPHI, por sus siglas en inglés).

¿Quién debe cumplir?

Todas las entidades cubiertas por HIPAA deben cumplir con la Regla de Seguridad. En general, los estándares, requisitos, y especificaciones de implementación de HIPAA aplican a las siguientes entidades cubiertas:

- **Proveedores del Cuidado de la Salud -** Cualquier proveedor medico u otro servicio de salud, o suplidor, que transmite cualquier información de salud en forma electrónica en conjunto con una transacción en la cual HHS a adoptado un estándar.
- **Planes de Salud -** Cualquier individuo o plan grupal que provee o paga el costo del cuidado de salud (e.g., distribuidor de seguro de salud y los programas de Medicare y Medicaid).

ESTANDARES DE SEGURIDAD DE HIPAA

Estándares de Seguridad: Reglas Generales

SALVAGUARDAS ADMINISTRATIVOS
- Proceso Gerencial de Seguridad
- Asignar las Responsabilidades de Seguridad
- Seguridad de los Trabajadores
- Gerencia al Acceso de Información
- Conocimiento de Seguridad y Adiestramiento
- Procedimientos de Incidentes de Seguridad
- Plan de Contingencia
- Evaluación
- Contratos de Socios y otros arreglos

SALVAGUARDAS FISICO
- Controles a las Facilidades de Acceso
- Uso del Área laboral
- Seguridad del Área Laboral
- Controles de los Medios y Dispositivos

SALVAGUARDAS TECNICOS
- Control de Acceso
- Controles de Contabilidad
- Integridad
- Autentificación de la Persona o de la Entidad
- Seguridad de Transmisión

REQUISITOS ORGANIZACIONALES
- Contratos de Socios de Negocio y Otros Arreglos
- Requisitos para Grupos de Planes de Salud

POLITICAS Y PROCEDIMIENTOS Y REQUISITOS DE DOCUMENTACION

- **Facilidad de Aprobación de Salud** - Un público o una entidad privada que procesa las transacciones del cuidado médico de otra entidad de un formato estándar a un formato no estándar, o viceversa.

- **Patrocinadores de la Tarjeta de Prescripción de Medicare** – Una entidad no gubernamental que ofrece un programa de descuento de medicina endosado bajo la ley de Modernización de Medicare. Seguirá habiendo esta cuarta categoría de la "entidad cubierta" en efecto hasta que el programa de tarjeta de medicina termine en el 2006.

Para más información sobre quien es una entidad cubierta bajo HIPAA, visite el sitio Web de la Oficina de los Derechos Civiles (OCR) en www.hhs.gov/ocr/hipaa o el sitio Web de CMS en http://www.cms.hhs.gov/hipaa/hipaa2. Una herramienta de ayuda para determinar si una organización es una entidad cubierta está disponible en el sitio Web de CMS, junto con un número de preguntas más frecuentes (FAQ, por sus siglas en inglés).

¿Porqué Seguridad?

Anterior a HIPAA, ningún sistema generalmente aceptado de estándares de seguridad o de requisitos generales para proteger la información de la salud existió en la industria del cuidado de la salud. Al mismo tiempo, las nuevas tecnologías se desarrollaban, y la industria del cuidado médico comenzó a moverse lejos de los procesos de papel y a confiar más fuertemente en el uso de computadoras para pagar las querellas, contestar preguntas de elegibilidad, proporcionar la información de la salud y de conducir un anfitrión en otras funciones basadas en lo clínico y administrativo. Por ejemplo, para proporcionar un acceso más eficiente a la información crítica de la salud, las entidades cubiertas están utilizando aplicaciones de bases-Web y otros "portales" que dan a los médicos, enfermeras, personal médico así como empleados administrativos más acceso a la información electrónica de la salud. Los proveedores también están utilizando aplicaciones clínicas tales como sistemas computarizados de entrada de pedido médico (CPOE), expedientes electrónicos de la salud (EHR), y radiología, farmacia, y sistemas de laboratorio. Los planes de salud están proporcionando acceso a las querellas y gerencia del cuidado, así como usos de aplicaciones de autoservicio para los miembros. Mientras que esto significa que la

HIPAA-Seguridad

Confidencialidad-
EPHI es accesible solamente por la gente autorizada y los procesos

Integridad-
EPHI no se altera ni se destruye de una manera desautorizada

Disponibilidad-
EPHI puede accesarse cuando se necesite por una persona autorizada

NOTA: La seguridad no es un proyecto de una sola vez, sino uno en movimiento, un proceso dinámico que creará nuevos retos hacia las entidades cubiertas y organizaciones según la tecnología cambie.

mano de obra médica puede ser más móvil y eficiente (es decir, los médicos pueden verificar expedientes y resultados de pruebas de los pacientes de dondequiera que estén) la subida del índice de la adopción de estas tecnologías crea un aumento en riesgos potenciales de la seguridad.

Mientras que el país se mueve hacia su meta de una Infraestructura Nacional de la Información de la Salud (NHII, por sus siglas en inglés), y el mayor uso de los expedientes electrónicos de la salud, protegiendo el secreto, la integridad, y la disponibilidad de EPHI llega a ser aún más críticas. Los estándares de la seguridad en HIPAA fueron desarrollados para dos propósitos primarios. Primero, y ante todo, la puesta en práctica de las salvaguardas apropiadas de la seguridad protege cierta información electrónica del cuidado médico que pueda estar en riesgo. En segundo lugar, protegiendo la información de la salud de un individuo, mientras que permite el acceso y el uso apropiado de esa información, promueve en última instancia el uso de la información electrónica de la salud en la industria - una meta importante de HIPAA.

Comparación entre La Regla de Privacidad y la Regla de Seguridad

La regla de privacidad fija los estándares para, entre otras cosas, que pueden tener acceso a PHI, mientras que la regla de la seguridad fija los estándares para asegurar eso solamente las que deben tener acceso a EPHI tendrán realmente acceso. Con el pasar ambas privacidad y las transacciones electrónicas y estándares de serie de código cumplir con las fechas límites para muchas entidades cubiertas se están enfocando en los requisitos de seguridad. En desarrollar la regla de seguridad, HHS eligió reflejar de cerca los requisitos de la regla final de Privacidad. La regla de privacidad le requiere a las entidades cubiertas tener en orden salvaguardas administrativas, físicas, y técnicas y implementar esas salvaguardas razonablemente. Como resultado, las entidades cubiertas que han implementado los requisitos de la regla de privacidad en sus organizaciones pueden encontrar que han tomado ya algunas de las medidas necesarias para cumplir con la regla de seguridad. Las distinciones primarias entre las dos reglas son:

- **Electrónico vs. oral y papel:** Es importante observar que la regla de privacidad se aplica a todas las formas de la información protegida de salud de los pacientes, ya sea electrónico, escrito, u oral. En contraste, la regla de seguridad cubre solamente la información protegida de la salud que está en forma electrónica. Esto incluye EPHI que se crea, se reciba, se mantenga o se transmita. Por ejemplo, EPHI se puede transmitir sobre el Internet, almacenado en una computadora, un CD, un disco, cinta magnética, u otros medios relacionados. La regla de la seguridad no cubre PHI que se transmita o se almacene en el papel o de forma oral.

- **"Salvaguarda "requisitos en la Regla de Privacidad:** La regla de privacidad contiene las provisiones en el 45 CFR 164,530(c) que requieren actualmente las entidades cubiertas para adoptar ciertas salvaguardas para PHI. Mientras que cumplir con la regla de seguridad no se requiere hasta 2005 para la mayoría de las entidades (2006 para los planes pequeños de salud), las entidades cubiertas que tomaron acción para implementar la regla de privacidad pueden haber realizado algunos requisitos de seguridad.

  Específicamente, el 45 CFR 164,530 (c) de la regla de privacidad indica:

NOTA: La OCR dentro de HHS supervisa y hace cumplir la Regla de Privacidad, mientras que CMS supervisa y hace cumplir el resto de los requisitos de la Simplificación Administrativa, incluyendo la Regla de Seguridad.

(c)(1) Estándar: salvaguardas. Una entidad cubierta debe tener en lugar salvaguardas administrativas, técnicas, y físicas apropiadas para proteger la privacidad de la información protegida de la salud.

(2) Especificación de Implementación: salvaguardas.

(i) Una entidad cubierta debe razonablemente salvaguardar la información protegida de la salud de cualquier uso o acceso intencional o no intencional o divulgación que esté en la violación de los estándares, especificaciones de implementación o otros requisitos de este subparte.

(ii) Una entidad cubierta debe razonablemente salvaguardar la información protegida de la salud para limitar los accesos accidentales o divulgaciones hechas conforme a un uso o a un acceso de otra manera permitido o requerido.

- La Regla de Seguridad provee más comprensivos requisitos de seguridad que el 45 CFR 164,530 (c) de la Regla de Privacidad e incluye un nivel del detalle no proporcionado en esa sección. Mientras que las entidades cubiertas comienzan iniciativas de planificación de cumplimiento de seguridad, deben considerar el conducir un gravamen de las iniciativas implementadas para cumplir con privacidad.

NOTA: Indique que leyes que son contrarias a la Regla de Privacidad y Regla de Seguridad se comparan con derecho preferente por los requisitos federales, a menos que una excepción específica se aplique. Para más información, vea 45 CFR.

Especificaciones de Implementación

Una "especificación de implementación" es una instrucción detallada adicional para poner en ejecución un estándar en particular. Cada sistema de salvaguardas se abarca de un número de estándares, que, en turnos, se abarcan generalmente de un número de especificaciones de implementación que sean requeridas o direccionales. Si una especificación de implementación es requerida, la entidad cubierta debe poner políticas y/o los procedimientos que resuelven los requisitos de la especificación de implementación. Si una especificación de la implementación es aplicable, entonces la entidad cubierta debe determinar si es una salvaguarda razonable y apropiada en su ambiente. Esto implica el analizar la especificación en referencia a la probabilidad de proteger el EPHI de la entidad contra amenazas anticipadas y peligros. Si la entidad cubierta elige no implementar una especificación aplicable basado en su tasación, debe documentar la razón y, si es razonable y apropiada, implementar una medida alterna equivalente. Vea el CFR 164.306(d)(ii)(B)(2) para más información.

NOTA:
Las especificaciones de implementación en la Regla de Seguridad es uno de dos "Requerido" o "Aplicable". Ver 45 CFR 164.306(d).

Para cada una de las especificaciones de implementación aplicable, la entidad cubierta debe hacer una de las siguientes:

- Implemente la especificación si es razonable y apropiada; o

- Si implementando la especificación no es razonable o apropiada –

    - Documente la razón que apoya la decisión y
    - Implemente una medida equivalente que sea razonable y apropiada y que lograría el mismo propósito o
    - No implemente la especificación de implementación aplicable o una medida equivalente, si el estándar puede todavía ser satisfecho y al implementar la especificación o una alternativa no sería razonable o apropiada.

NOTA: Aplicable no significa opcional.

Si una especificación de implementación aplicable dada se determina ser razonable y apropiada, la entidad cubierta debe considerar las opciones para implementarla. La decisión con respecto a que medidas de seguridad implementar en dirigir los estándares y las especificaciones de implementación dependerán de una variedad de factores, incluyendo:

- **El análisis de riesgo de la entidad -** ¿Qué circunstancias actuales dejan la entidad abierta al acceso desautorizado y divulgación de información electrónica de la salud?
- **El análisis de seguridad de la entidad -** ¿Qué medidas de seguridad están ya en lugar o se podrían razonablemente poner en lugar?
- **El análisis financiero de la entidad -** ¿Cuánto costará la implementación?

NOTA: Para más información sobre Análisis de Riesgo, vea el documento 6 de esta serie, "Fundamentos de Análisis de Riesgo y de Manejo de Riesgo."

Descripción del Proceso

La tabla de las especificaciones requeridas y direccionales de implementación incluidas en contornos de este papel los estándares y las especificaciones de la puesta en práctica en la seguridad gobiernan. Para cumplir con la regla de seguridad, todas las entidades cubiertas deben utilizar el mismo acercamiento básico. El proceso debe, en un mínimo, requerir a entidades cubiertas:

- **Determinar la seguridad, los riesgos, y brechas actuales.**
- **Desarrollar un plan de implementación.**

    - **Lea la Regla de Seguridad.** Una entidad cubierta debe repasar todos los estándares y especificaciones de implementación. La matriz al final de la Regla de Seguridad es un recurso excelente al desarrollar un plan de implementación, y es incluida en el final de este documento.

- **Revise las especificaciones de implementación direccionales.** Para cada especificación dirección hable de implementación, una entidad cubierta debe determinar si la especificación de implementación es razonable y apropiada en su ambiente. Una entidad cubierta necesita considerar un número de factores al tomar las decisiones para cada especificación dirección hable de implementación. .

- **Determine las medidas de seguridad.** Una entidad cubierta puede utilizar cualquier medida de seguridad que la permita razonablemente y apropiadamente implementar los estándares y especificaciones de implementación. (Véase el 45 CFR 164.306(b), la flexibilidad del acercamiento).

- **Implemente soluciones.** Una entidad cubierta debe implementar las medidas de seguridad y las soluciones que son razonables y apropiadas para la organización.

- **Documente las decisiones.** Una entidad cubierta debe documentar su análisis, decisiones y el análisis de razonamiento para sus decisiones.

- **Valore de nuevo periódicamente.** Una entidad cubierta debe repasar y poner al día periódicamente sus medidas de seguridad y documentación en respuesta a los cambios ambientales y operacionales que afectan la seguridad de su EPHI.

NOTA: La Regla de Seguridad requiere que la entidad cubierta documente el análisis razonado para muchas de sus decisiones de seguridad.

Estándares flexibles y escalables

Los requisitos de seguridad fueron diseñados para ser tecnología neutral y escalable desde el más grande de los planes de salud hasta el más pequeño de las prácticas del proveedor. Las entidades cubiertas encontrarán que cumplir con la regla de seguridad requerirá una evaluación de cuáles son las medidas de seguridad actualmente en lugar, un exacto y cuidadoso análisis de riesgo, y una serie de soluciones documentadas derivadas de un número de factores complejos únicos a cada organización.

A partir de 45 CFR 164,306(b) Factores que deben ser considerados:

- El tamaño, la complejidad y las capacidades de la entidad cubierta.
- La infraestructura de la entidad cubierta, el hardware, y las capacidades del sistema de computadora de seguridad.
- Los costos de medidas de seguridad.
- La probabilidad y los riesgos potenciales críticos de EPHI.

HHS reconoce que cada entidad cubierta es única y varía de tamaño y recursos, y que no hay sistema totalmente seguro. Por lo tanto, los estándares de seguridad fueron diseñados para proporcionar pautas a todos los tipos de entidades cubiertas, mientras que les producían flexibilidad con respecto de cómo poner los estándares en implementación. Las entidades cubiertas pueden utilizar medidas de seguridad apropiadas que les permiten razonablemente implementar un estándar. En decidir qué medidas de seguridad utilizar, debe considerar una entidad cubierta su tamaño, capacidades, los costos de las medidas de seguridad específicas y el impacto operacional.

Por ejemplo, se esperará que las entidades cubiertas balanceen los riesgos del uso o del acceso inadecuado de EPHI contra el impacto de varias medidas protectoras. Esto significa que prácticas más pequeñas y menos sofisticadas pueden no poder implementar seguridad de la misma manera y en el mismo costo que entidades grandes, complejas. Sin embargo, el costo solamente no es una razón aceptable de no implementar un procedimiento o medida.

NOTA: Los estándares de seguridad no dictan ni especifican el uso de tecnologías específicas.

Estándares de Tecnología Neutral

Por los últimos años, la aparición de nuevas tecnologías ha conducido muchas iniciativas del cuidado médico. Con mejoras de la tecnología y el crecimiento rápido en la industria del cuidado médico, la necesidad de estándares neutrales de tecnología flexible es crítica para una implementación de éxito. Cuando la regla final de seguridad fue publicada, los estándares de seguridad fueron diseñados para ser "tecnología neutral" para acomodar cambios. La regla no prescribe el uso de tecnologías específicas, de modo que la comunidad del cuidado médico no sea limitada por los sistemas y/o programas de computadora que pueden llegar a ser obsoletos. HHS también reconoce que las necesidades de seguridad de entidades cubiertas pueden variar significativamente. Esta flexibilidad dentro de la regla permite a cada entidad elegir tecnologías para resolver lo más mejor posible sus necesidades específicas y para cumplir con los estándares.

Estándares de Seguridad

Los estándares de seguridad se dividen en las categorías de salvaguardas administrativas, físicas, y técnicas. Las definiciones reguladoras de las salvaguardas se pueden encontrar en la regla de seguridad en el 164,304 de 45 CFR.

- **Salvaguardas Administrativos**: En general, éstas son las funciones administrativas que se deben implementar para resolver los estándares de seguridad. Éstos incluyen la asignación o delegación de responsabilidad de seguridad a un individuo, los requisitos de adiestramiento, y/o la documentación de decisiones. (para más información, vea el 164,308 de 45 CFR y el documento 2 de esta serie titulada los "estándares de seguridad-salvaguardas administrativos".)

- **Salvaguardas físicos:** En general, éstos son los mecanismos requeridos para proteger sistemas electrónicos, el equipo y los datos que llevan a cabo, contra amenazas, peligros para el medio ambiente y la intrusión desautorizada. Incluyen el acceso de restricción a la información electrónica de la salud y la retención de reservas de las computadoras fijas. (para más información, vea el 164,310 y el documento 3 de 45 CFR "los estándares de seguridad - salvaguardas físicos".)

- **Salvaguardas Técnicos:** En general, éstos son principalmente todos los procesos automatizados usados para proteger datos y para controlar el acceso a los datos. Incluyen los controles de la autentificación para verificar que autorizan a la persona que firma sobre una computadora a tener acceso a ese EPHI, o cifrando y descifre datos mientras que se está almacenando y/o se está transmitiendo.

Una lista completa de las salvaguardas administrativas, físicas, y técnicas y incluyendo requisitos requeridos y direccionales de especificaciones de implementación es incluida al final de este documento. Además de las salvaguardas, la Regla de Seguridad también contiene varios estándares y especificaciones de

implementación en práctica que traten requisitos de organizaciones, así como políticas y procedimientos y requisitos de documentación. (Véase el 164,314 de 45 CFR y el 164,316 de la Regla de Seguridad.)

Recursos

Los papeles restantes en esta serie tratarán asuntos específicos relacionados con la Regla de Seguridad. Las entidades cubiertas deben periódicamente verificar el sitio Web de CMS en http://www.cms.hhs.gov/hipaa/hipaa2 para información adicional y recursos mientras trabajan con el proceso de implementación de seguridad. Hay muchas otras fuentes de información disponibles en el Internet. Las entidades cubiertas pueden también verificar con otras organizaciones profesionales locales y nacionales del cuidado médico, tales como proveedores nacionales y asociaciones de plan de salud.

¿Necesita más información?

Visite el sitio Web de CMS en: http://www.cms.hhs.gov/hipaa/hipaa2 para los últimos documentos de seguridad, listas de cotejo, información por Internet (webcasts) y anuncios de próximos eventos.

Llame a la línea de ayuda de CMS al 1-866-282-0659, use el HIPAA TTY 877-326-1166, o el sistema de correo electrónico en: askhipaa@cms.hhs.gov

Visite el sitio Web de La Oficina de los Derechos Civiles, http://www.hhs.gov/ocr/hipaa, para las ultimas guías, preguntas más frecuentes (FAQ, por sus siglas en inglés), documentos y otra información de la Regla de Privacidad.

Matriz de la Ley de Seguridad (Apéndice A de la Ley de Seguridad)

SALVAGUARDAS ADMINISTRATIVOS			
Estándares	**Secciones**	**Especificaciones de Implementación (R)= Requerido, (A)=Aplicable**	
Proceso de Manejo de Seguridad	164.308(a)(1)	Análisis de Riesgo	**(R)**
		Riesgo de Manejo	**(R)**
		Política de Sanción	**(R)**
		Revisión de la Actividad de los Sistemas de Información	**(R)**
Asignación de Responsabilidad de Seguridad	164.308(a)(2)		
Seguridad de La Fuerza laboral	164.308(a)(3)	Autorización y/o Supervisión	**(A)**
		Procedimientos de Aprobación para La Fuerza Laboral	**(A)**
		Procedimientos de Terminación	**(A)**
Manejo del Acceso a la Información	164.308(a)(4)	Aislamiento de funciones de Las Casas de Aprobación	**(R)**
		Autorización de Acceso	**(A)**
		Establecimiento y Modificación del Acceso	**(A)**
Conocimiento y Adiestramiento de Seguridad	164.308(a)(5)	Avisos de Seguridad	**(A)**
		Protección contra sistemas de computadora maliciosos	**(A)**
		Monitoreo de Registro	**(A)**
		Manejo de Claves	**(A)**
Procedimientos para los Incidentes de Seguridad	164.308(a)(6)	Reporte y Respuesta	**(R)**
Plan de Contingencia	164.308(a)(7)	Plan de Copia de Datos	**(R)**
		Plan de Recuperación de Desastres	**(R)**
		Plan de Operación a Modo de Emergencia	**(R)**
		Procedimientos de Prueba y Revisión	**(A)**
		Análisis de Critico de Aplicaciones y Datos	**(A)**
Evaluación	164.308(a)(8)		
Contratos de Acuerdos Comerciales y Otros Arreglos	164.308(b)(1)	Contrato escrito y Otros Acuerdos	**(R)**

SALVAGUARDAS FISICOS			
Estándares	**Secciones**	**Especificaciones de Implementación (R)= Requerido, (A)=Aplicable**	
Control de Acceso a las Facilidades	164.310(a)(1)	Operaciones de Contingencia	**(A)**
		Plan de Seguridad de la Facilidad	**(A)**
		Procedimiento de Validación y Control de Acceso	**(A)**
		Registro de Mantenimiento	**(A)**
Uso de Estaciones de Trabajo	164.310(b)		
Seguridad de Estaciones de Trabajo	164.310(c)		**(R)**
Controles de Medios y Equipos	164.310(d)(1)	Eliminación	**(R)**
		Re-uso de Medios	**(R)**
		Contabilidad	**(A)**
		Almacenamiento y Copia de Datos	**(A)**

SALVAGUARDAS TECNICOS			
Estándares	**Secciones**	**Especificaciones de Implementación (R)= Requerido, (A)=Aplicable**	
Controles de Acceso	164.312(a)(1)	Identificación Único del Usuario	**(R)**
		Procedimientos de Acceso de Emergencia	**(R)**
		Salida Automática del Sistema	**(A)**
		Cifrado y Descifrado	**(A)**
Controles de Auditoria	164.312(b)		
Integridad	164.312(c)(1)	Mecanismos para Autenticar la Información de Salud Protegida Electrónica	**(A)**
Autenticación de Entidades o Personas	164.312(d)		
Seguridad en la Transmisión	164.312(e)(1)	Controles de Integridad	**(A)**
		Cifrado	**(A)**