RadiologyInfo.org
Para pacientes

Privacidad de la información médica

Resumen

- Usted tiene el derecho a decidir si quiere compartir su información médica confidencial.
- Los grupos del sector médico deben mantener su información médica electrónica en forma segura.
- Si usted sospecha que alguien ha tenido acceso no autorizado a su información, contacte inmediatamente a su proveedor de servicios médicos.

Su información médica está almacenada en formato electrónico. Existen muchas reglas y regulaciones (incluyendo la Ley de transferencia y seguridad de los seguros médicos, HIPAA) que existen para proteger su información médica.

Los médicos necesitan acceder a su información médica para tomar decisiones rápidas importantes sobre sus cuidados médicos. Sin embargo, usted tiene el derecho a decidir si ellos pueden acceder a su información o pueden compartirla con otros.

Los grupos médicos han desarrollado métodos para proteger su información médica. A medida que la tecnología mejora, los grupos médicos también están mejorando las formas en las que guardan su formación de forma segura.

Médicos deben ayudar a proteger su información. Ellos deben documentar todo uso de la información, compartir sus normas de privacidad y seguridad con usted, informar sobre cualquier brecha o pérdida de información. Contacte a la oficina de su médico inmediatamente si usted sospecha que alguien está usando su información de forma no adecuada.

¿Qué es la seguridad de la información médica electrónica?

Los grupos médicos almacenan imágenes, resultados médicos, notas de los médicos, medicamentos, alergias, y otras informaciones electrónicas. Los médicos tienen la responsabilidad primaria de “no dañar”. Los grupos médicos almacenan imágenes, resultados médicos, notas de los médicos, medicamentos, alergias, y otras informaciones electrónicas. Los médicos tienen la responsabilidad primaria de “no dañar”. Esta responsabilidad incluye proteger su información, su privacidad, y su confidencialidad. La seguridad de la información médica de los pacientes detalla los pasos que los empleados del sector médico deben seguir para “proteger información de la salud” (PHI). La seguridad también se refiere al mantenimiento de la integridad de la información médica electrónica. Asegura que aquellos que lo necesiten, puedan acceder a su información médica para brindarle cuidados médicos. El gobierno federal regula el manejo de los archivos electrónicos y su información médica protegida.

Las actividades de investigación y de educación también deben cumplir con los requerimientos de privacidad y seguridad. Las instituciones deben proteger la privacidad de su información médica, al mismo tiempo que permiten el acceso razonable de los investigadores, educadores, o becarios.

¿Qué es la privacidad del paciente?

La privacidad del paciente es su derecho a decidir cuándo, cómo, y hasta qué punto otros pueden acceder a su información médica protegida (PHI). La privacidad del paciente mantiene la confidencialidad y solamente comparte su información con aquellos que la necesitan para brindar servicios médicos. Si su información es utilizada con fines de investigación, los investigadores deben requerir aprobación de consejo de investigadores de la institución local (IRB). Esto podría incluir el hacer que esa información sea anónima antes de utilizarla para llevar a cabo las investigaciones.

¿Por qué son importantes la seguridad y la privacidad del paciente?

La seguridad de la información médica electrónica puede afectar la calidad de los cuidados del paciente y los derechos del paciente. También puede impactar las prácticas laborales y las responsabilidades legales de los profesionales de la salud. Los médicos pueden tomar las mejores decisiones para sus cuidados si pueden acceder a su historia médica completa. La falta de acceso puede demorar decisiones importantes y dañar su salud. Los métodos de protección deben mantener su información privada y confidencial y al mismo tiempo permitir que individuos autorizados puedan acceder a la misma rápidamente.

¿Qué están haciendo los profesionales de la radiología para asegurar las imágenes médicas y la información del paciente?

Los radiólogos son uno de los primeros médicos que adoptaron las imágenes médicas digitales y la información médica electrónica. Ellos reconocen los beneficios de estas tecnologías y están trabajando para eliminar los riesgos. Este trabajo se realiza a través de grupos como la Radiological Society of North America (RSNA) (https://www.radiologyinfo.org/es/info/about-rsna) , American College of Radiology (ACR) (https://www.radiologyinfo.org/es/info/about-acr) ,y la Society for Imaging Informatics in Medicine (SIIM) (https://siim.org/) . Juntos, estos líderes en el campo de la medicina están desarrollando estándares y creando normas para asegurar que su información radiológica permanezca segura pero que pueda ser fácilmente accesible para que usted reciba cuidados médicos de alta calidad.

¿Cuáles son las responsabilidades del radiólogo y del paciente?

Los radiólogos trabajan con los profesionales informáticos para proteger su información, privacidad, confidencialidad, e integridad. Los médicos deben documentar sus normas de privacidad y seguridad y compartirlas con usted. Todos los empleados deben ser entrenados con respecto a las normas de seguridad. Estas normas deben incluir copias de seguridad para los sistemas de computación, mantenimiento, almacenamiento adecuado de la información, fallo de los sistemas y planes de recuperación, reportes de incidentes, y solución de cuestiones relacionadas con la seguridad. El no cumplir con las regulaciones estatales y federales con respecto a la información médica electrónica protegida (ePHI) resulta en sanciones financieras y/o criminales.

En su calidad de paciente, usted tiene el derecho de hablar con su médico de forma confidencial y de tener su información protegida. Usted decide si la quiere compartir, excepto cuando es requerido por la ley o en caso de una emergencia.

¿Qué debería hacer si creyera que alguien está accediendo a su información médica electrónica de forma inadecuada?

Si usted cree que alguien está usando incorrectamente su información médica, contacte al consultorio de su médico inmediatamente, las reglas federales detallan pasos que los proveedores médicos deben seguir para investigar, informar, y responder al uso no autorizado de su información médica que comprometiera su privacidad. Si su información ha sido expuesta, su proveedor médico podría brindarle una descripción del incidente y detallar cuáles son los pasos que usted debería seguir para protegerse. El proveedor médico también debería informarle acerca de qué harán para recuperar la pérdida y evitar fallos de seguridad en el futuro. Este informe debe identificar a quien usted debería contactar si tuviera alguna pregunta con respecto al fallo de seguridad.

¿Cómo se mantiene segura y privada la información médica?

Varios sistemas de seguridad protegen su privacidad, seguridad, e integridad de su información. Al mismo tiempo, estos sistemas de seguridad permiten a los médicos el acceso para que puedan brindarle sus cuidados médicos. Los sistemas de seguridad físicos incluyen:

- La utilización de aparatos de almacenamiento codificados o encriptados

- La restricción física del acceso solamente al personal autorizado
- La preservación de copias y la creación de copias de seguridad
- El mantenimiento de protocolos de emergencia
- El desecho adecuado de aparatos obsoletos

Las medidas de seguridad técnicas incluyen firewalls y los modos seguros de transmisión para la comunicación. Los mismos incluyen redes virtuales privadas (VPN), y protocolos de capa de conexión segura (SSL), y técnicas de encripción.

Las medidas de seguridad administrativas incluyen:

- La documentación de las normas de seguridad del departamento
- El entrenamiento del personal con respecto a las normas de seguridad
- La realización de auditorias de los registros del sistema relacionados con la identificación y actividad de los usuarios
- Hacer respetar las normas de almacenado electrónico de los datos y las copias de seguridad
- Brindar métodos específicos para informar sobre incidentes, y resolver problemas de seguridad
- Documentar la rendición de cuentas, sanciones, y acciones disciplinarias por cualquier violación de las normas y procedimientos
- Aprobación del IRB para cualquier estudio que involucre información médica protegida o sujetos humanos

Los registros médicos electrónicos (EMRs) deben incluir lo siguiente en sus normas y procedimientos de seguridad:

- autorización
- autentificación
- disponibilidad
- confidencialidad
- integridad de los datos
- no repudio.

Los métodos de control de autorización/acceso incluyen bases de datos de acceso único o listas asignando los derechos y privilegios de acceso de los usuarios. Esto también incluye cierre de sesión automático luego de cierto periodo de inactividad. Esto ayuda a prevenir el acceso de usuarios no válidos. También se podrían utilizar el cambio frecuente de las claves de acceso y de los controles físicos de acceso (tales como las tarjetas de identificación con chip).

La autenticación verifica su identidad en el sistema de computación utilizando palabras clave de acceso, certificados digitales, tarjetas inteligentes, y datos de biometría, y sistemas multi-factoriales. La autenticación solamente verifica su identidad. No define los recursos a los que puede acceder.

El EMR debe estar continuamente disponible, y administradores del Sistema deben defenderlo contra varias amenazas. Ellos deben brindar copias de seguridad para sus sistemas (hardware duplicado, archivos de datos, electricidad, y redes de sistemas). También deben mantener los servidores seguros desde el punto de vista físico y defenderlos de virus informáticos y de la piratería informática.

Confidencialidad significa que cualquier acceso no autorizado de sus datos médicos será bloqueado.

Es esencial mantener la integridad de los datos cuando se transfiere información. Esto se logra mediante la verificación de qué la información ha llegado de la misma forma que fue enviada y no ha sido modificada de ninguna forma. El personal de informática utiliza una variedad de métodos para mantener la integridad de los datos y detectar cualquier intento de modificar los datos, tales como firmas digitales.

El no repudio ofrece un informe de la transacción. Esto asegura que un mensaje transferido haya sido enviado y recibido por los sujetos que dicen haber enviado y recibido los datos. Los métodos incluyen firmas digitales y registros de todas las actividades de los usuarios.

Si usted aún tiene preguntas sobre cómo se protege esta información privada, por favor hable con su médico.

Condiciones de uso:

Todas las secciones del sitio fueron creadas bajo la dirección de un médico experto en el tema. Toda la información que aparece en este sitio web fue además revisada por un comité de ACR-RSNA formado por médicos peritos en diversas áreas de la radiología.

Sin embargo, no podemos asegurar que este sitio web contenga información completa y actualizada sobre ningún tema particular. Por lo tanto ACR y RSNA no hacen declaraciones ni dan garantías acerca de la idoneidad de esta información para un propósito particular. Toda la información se suministra tal cual, sin garantías expresas o implícitas.

Visite el Web site de RadiologyInfo en http://www.radiologyinfo.org/sp para visión o para descargar la información más última.

Nota: Las imágenes se muestra para fines ilustrativos. No trate de sacar conclusiones comparando esta imagen con otras en el sitio. Solamente los radiólogos calificados deben interpretar las imágenes.

Copyright