



**Familiarícese con
los Hechos sobre la
Información Electrónica
de la Salud**

*Es Segura, Privada
y Accesible.*



Información Electrónica sobre la Salud: Es Segura, Privada y Accesible

Parece que la mayoría de la información que actualmente usted necesita está disponible electrónicamente. ¿Qué tal si su expediente médico estuviera también disponible electrónicamente? El gobierno federal ha fijado una meta para que la mayoría de los americanos tengan sus expedientes médicos en forma electrónica antes del 2014.

¿Qué es un expediente de salud electrónico (EHR, por sus siglas en inglés)? Es una versión computarizada de su historial médico. Muchos médicos en Georgia están en el proceso de convertir los tradicionales expedientes médicos escritos en EHRs. Con los EHRs, su información médica es electrónicamente almacenada y puede ser leída y compartida con otros médicos que lo están tratando. Cuando los médicos utilizan los EHRs pueden ver inmediatamente todo su historial médico incluyendo los resultados de exámenes, alergias, y medicamentos que este tomado, de tal forma que en una emergencia se ahorrarían tiempo y dinero no teniendo que repetir exámenes médicos costosos. Otra ventaja de los EHRs es que la información de su estado de salud es segura y privada.

Pronto los doctores y proveedores de salud con los EHRs podrán tener a su alcance toda una red para el Intercambio de Información sobre la Salud de los pacientes (HIE por sus siglas en Inglés). La HIE permite que los EHRs sean compartidos entre los proveedores de salud, los pacientes y otras personas autorizadas. Por ejemplo, su cardiólogo podría obtener electrónicamente el expediente médico de su doctor o proveedor de salud primario haciendo su tratamiento más rápido y más seguro.

Seguridad y Privacidad

Mientras que los EHRs hacen más conveniente el acceso a su expediente médico, su privacidad sigue siendo una prioridad. Usted tiene derecho a saber y a tener información sobre su estado de salud y de autorizar el acceso a la información que es confidencial tal como droga, alcohol o tratamientos de salud mental a los proveedores de salud de su elección.

Como mucha gente, usted puede estar preocupado(a) por la seguridad de los EHRs. Pero los EHRs deben cumplir con las normas de confidencialidad del seguro médico de 1996 conocido como (HIPAA, por sus siglas en Inglés) que son unas normas de Privacidad y Seguridad y requiere que los proveedores de salud tomen las medidas apropiadas y razonables para proteger la privacidad de su información y la distribución de esa información esté limitada a la mínima cantidad necesaria de profesionales de salud para que realicen su trabajo.

A diferencia de los expedientes médicos escritos, los EHRs pueden colocarse en un sitio seguro de modo que solamente los individuos autorizados puedan tener acceso a su información. Otras formas de seguridad diseñados para proteger su información pueden incluir:

- Un código de identificación del usuario (contraseña) y un número de identificación personal (PIN) como requisitos para tener acceso
- Un sistema de seguimiento electrónico se podría utilizar para documentar y para supervisar quién ha mirado su información de salud

Seguridad del Paciente

Los EHRs pueden mejorar la seguridad del paciente ayudando a los proveedores de salud a identificar reacciones adversas a los medicamentos, alergias u otras complicaciones. Los proveedores también pueden enviar recordatorios sobre exámenes o pruebas programadas, revisar los resultados de los exámenes y establecer mejores perfiles del historial médico de cada paciente. Los errores médicos pueden reducirse mientras que la calidad de atención médica es mejorada.



Ventajas

Las ventajas de los EHRs son numerosas. ¡Si usted siempre se preguntaba cómo es que el farmacéuta descifró una prescripción que su médico escribió, usted no esta solo(a)! Una de las muchas ventajas de guardar sus datos médicos electrónicamente es que sus archivos serán más fáciles de leer. Nadie mas tendrá que descifrar notas manuscritas – los errores pueden ser evitados.

Otras ventajas son:

- Los EHRs permiten una recuperación más rápida y más completa de la información de la salud del paciente. Un médico verá inmediatamente los tratamientos que actualmente recibe, los medicamentos, alergias o un diagnostico anterior
- Los EHRs pueden ser recuperados. Si ocurriera un desastre natural tal como el huracán Katrina, los EHRs serían archivados y se salvarían, mientras que seria más probable que los archivos escritos se perdieran o se dañaran
- Los EHRs se pueden proteger de tal forma que solo las personas autorizadas puedan tener acceso a ellos, haciendo que sea mas fácil mantenerlos seguros y privados que los expedientes escritos

Como consumidor del sistema de salud, usted tiene el derecho a tener acceso a su información personal de salud. Los proveedores de salud deben cumplir con este derecho:

- Solicitando una copia de sus expedientes de salud
- Solicitando que se hagan las correcciones a sus expedientes

Hay circunstancias en las que un proveedor de salud no necesita solicitar su permiso para tener acceso o compartir a su información, por ejemplo:

- Para proporcionarle tratamiento médico
- Para pagar a los proveedores de salud por su cuidado
- Para proteger la salud de público, tal como información sobre brotes de gripe (influenza) en su área
- Para informes solicitados por la policía, tales como información sobre heridas de bala

Para más información sobre seguridad y privacidad de los EHRs, vaya por favor al siguiente portal (Website): [georgiahealthinfo.gov](https://www.georgiahealthinfo.gov) y haga clic sobre **Health Information Security and Privacy** (Información sobre Seguridad y Privacidad de la Salud) en la pagina principal.

Esta publicación ha sido posible realizarla gracias a la colaboración de la Información sobre Seguridad y Privacidad (HISPC por sus siglas en inglés) un contrato dirigido y manejado por la Oficina de Coordinación Nacional para la Salud IT (ONC por sus siglas en inglés). Ni el HISPC ni el ONC son responsables por el mal uso o por la violación de derechos de autor con respecto a esta publicación.