CONSEJOS DE SEGURIDAD PARA LA ATENCIÓN VIRTUAL *de los pacientes*

La atención virtual ofrece a los pacientes comodidad, flexibilidad y costos reducidos. Para asegurarnos de que su información esté segura, tenga en cuenta las siguientes medidas de seguridad.

Descargo de responsabilidad: *La ciberseguridad es un tema cambiante. Esta infografía contiene sugerencias generales. Para obtener consejos específicos, consulte a su asesor legal o especialista en seguridad informática de la salud.*

PRACTIQUE UNA ADECUADA HIGIENE CIBERNÉTICA

¿Qué es la higiene cibernética? Al igual que lavarse las manos y dormir lo suficiente, una adecuada higiene cibernética es un conjunto de buenas prácticas para mantener su información digital saludable y segura.

Utilice contraseñas seguras

Una contraseña segura utiliza 12 o más caracteres. Es única para cada cuenta y combina letras mayúsculas, minúsculas y símbolos.

Utilice software de seguridad en su dispositivo

El software de cortafuegos, antivirus y antimalware ayuda a proteger su red y sus dispositivos de actividades dañinas.

Utilice un router seguro

Si utiliza una conexión inalámbrica a Internet, verifique que el router sea seguro y esté protegido con una contraseña establecida por usted.

Actualice

Instale las respectivas actualizaciones de software para disponer de parches de seguridad para:

- Sistemas operativos en teléfonos, tabletas y computadoras
- Navegadores de Internet
- Routers y módems

Cierre el ciclo

Cierre sesión en sus cuentas, cierre aplicaciones y desactive el Bluetooth, el micrófono y la cámara una vez que se complete la sesión de atención virtual.

PRIVACIDAD

Cuando participe en la atención virtual, es esencial saber quién verá su pantalla y escuchará sus conversaciones.

Encuentre una ubicación correcta

Elija un lugar privado para ver su información de salud personal y sus visitas virtuales.

Utilice una conexión segura

No utilice Wi-Fi público para la atención virtual o para acceder a información confidencial.

Utilice el Bluetooth prudentemente

Utilice únicamente dispositivos o auriculares conectados por Bluetooth para la atención virtual en entornos privados.

Invitados exclusivos

Pídale a su proveedor que identifique a cualquier otra persona que esté en la sala con ellos o corta distancia.

A su vez, infórmele a su proveedor si las personas que están en la sala de accesos con usted tienen autorización para estar allí.

Inspeccione su entorno

Apague los dispositivos de grabación y elimine cualquier cosa que muestre información personal que no sea necesaria durante su consulta virtual.

INFÓRMESE SOBRE LAS POLÍTICAS

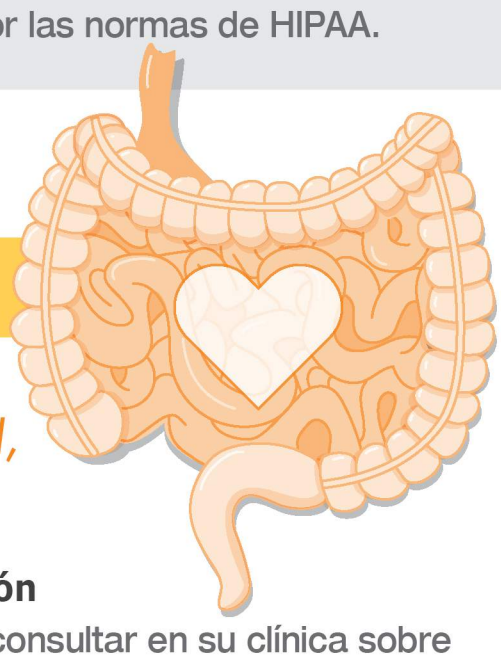
La política federal, estatal y de la clínica le ofrece algunas protecciones de privacidad y seguridad, pero es posible que no se apliquen a todas las herramientas digitales relacionadas con su atención. Solicite las políticas y consulte si tiene dudas.

Políticas de su proveedor de atención médica

Lea sobre las prácticas actualizadas de privacidad y seguridad de su proveedor de atención médica.

Políticas de sus aplicaciones y dispositivos

No asuma que todas las aplicaciones y herramientas digitales de mHealth están protegidas por las normas de HIPAA.



CONFÍE EN SU INSTINTO

A menudo, nuestros sentidos nos advierten de posibles dificultades. Si algo parece fuera de lugar o demasiado bueno para ser verdad, verifique la fuente antes de comunicarse con cualquier correo electrónico, correo de voz o persona.

Analice antes de hacer clic

Las estafas por correo electrónico son comunes.

Si algo no parece estar bien, no haga clic.

De su opinión

No dude en consultar en su clínica sobre sus medidas de seguridad y protección o compartir sus opiniones.

El California Telehealth Resource Center (CTRC) y los recursos y actividades producidos o respaldados por el CTRC son posibles gracias a la concesión número GA5RH37469 de la Oficina para los Avances de la Telesalud, Administración de Recursos y Servicios de Salud, DHHS. La información o el contenido y las conclusiones aquí indicadas corresponden al CTRC. No deberán interpretarse como la posición o política oficial de HRSA, HHS o el gobierno de los EE. UU. No deberán inferirse como aprobaciones oficiales de ningún tipo, por parte de alguna de estas entidades.