Preguntas frecuentes (FAQ) para la seguridad en la atención virtual de pacientes

1. ¿Cómo sé que mi consulta por video será segura?

Es esencial saber que su proveedor de atención médica tiene la responsabilidad de proteger su privacidad durante un encuentro por video. Una de las cosas más importantes que hizo la ley de transferencia y responsabilidad de los seguros médicos (HIPAA) fue exigir la protección y el manejo seguro de determinada información, conocida como Información Médica Protegida. Por ejemplo, su proveedor de atención médica deberá contar con sistemas para garantizar que solo las personas autorizadas tengan acceso a su información médica. Esto es cierto ya sea que la información esté en físico o en un sistema informático. Las regulaciones de HIPAA también se aplican a cualquier información transmitida por Internet, incluidas las consultas por video.

Para cumplir con HIPAA, su proveedor de atención médica deberá utilizar una solución virtual que cumpla con los estrictos estándares de HIPAA. Comuníquese con su proveedor de atención médica si tiene alguna pregunta o inquietud sobre la privacidad y la seguridad de la información compartida durante su sesión de telesalud.

2. ¿Cuáles son las medidas de seguridad de la atención virtual?

HIPAA exige que los proveedores integren el cifrado y otras medidas de seguridad en sus interacciones con los pacientes. Todos los profesionales médicos u organizaciones de atención médica que ofrecen servicios remotos a pacientes en sus hogares o en centros comunitarios deberán cumplir con las pautas de HIPAA. Las normas de privacidad y seguridad de HIPAA brindan protección para la información personal de salud. La norma de privacidad de HIPAA establece límites en el uso y la divulgación de información personal de salud, y su norma de seguridad establece medidas de seguridad técnicas, físicas y administrativas que protegen la información electrónica personal de salud. Por ejemplo, el cifrado de datos almacenados y en tránsito es una "especificación de implementación direccionable" según la norma de seguridad, lo cual significa que se espera que las entidades cubiertas por HIPAA realicen el cifrado a menos que no sea "razonable y adecuado" hacerlo de esa forma. Además, las regulaciones establecen que los proveedores deberán adoptar protocolos de gestión de identidad y controles de acceso.

3. ¿Cuáles son los riesgos de utilizar Wi-Fi público durante mi teleconsulta?

Los puntos de acceso de Wi-Fi en cafeterías, bibliotecas, aeropuertos, hoteles y otros lugares públicos son convenientes, pero a menudo no son seguros. Requerir una contraseña para iniciar sesión no significa necesariamente que sus actividades en línea estén encriptadas. El Wi-Fi público puede mantenerlo vulnerable por diferentes razones. Una de ellas tiene que ver con el protocolo de cifrado que utilizan algunas redes inalámbricas.

Otra implica la posibilidad de unirse a un punto de acceso Wi-Fi fraudulento o no autorizado. No recomendamos el uso de puntos de acceso Wi-Fi públicos para realizar consultas virtuales. Considere utilizar sus datos móviles en lugar de Wi-Fi como alternativa. (Nota: Es posible que se le cobre por el uso de datos según el plan de su dispositivo móvil).

4. ¿Cuáles son algunas amenazas de seguridad comunes?

- Ataques de phishing
  Los ataques de phishing ocurren cuando un intruso se hace pasar por un contacto confiable. Un intento de phishing puede incitar a un usuario a hacer clic en un enlace malicioso; descargar un archivo malicioso; o proporcionar acceso a información confidencial, detalles de cuentas o credenciales.
- Ataques de malware
  El malware abarca una variedad de amenazas cibernéticas, incluidos troyanos y virus. Todos involucran un código malicioso que los piratas informáticos crean para obtener acceso a la red, robar información o eliminar datos en las computadoras. El malware generalmente proviene de descargas de sitios web maliciosos, correos electrónicos no deseados o conexión con otros dispositivos infectados.
- Ransomware
  El ransomware es un tipo específico de malware que infecta y restringe el acceso a una computadora hasta que se realice el pago de un rescate. El ransomware generalmente se envía a través de correos electrónicos de phishing y toma ventaja de los puntos débiles sin parches en el software.
- Ataque "Man in the Middle" (MitM)
  En este caso, un intruso establece una posición entre el remitente y el destinatario de los mensajes electrónicos e intercepta esos mensajes, quizás cambiándolos en tránsito. El remitente y el destinatario creen que se están comunicando directamente entre sí.

5. ¿De qué formas el software antivirus y antimalware protegen mi computadora?

Beneficios del software antivirus y antimalware

- Beneficios del software antivirus y antimalware
- Detectan y protegen contra malware, virus y otro software dañino en tiempo real
- Contienen componentes dinámicos de detección y respuesta antiransomware y anti-exploit
- Bloquean los intentos de piratería y phishing
- Ofrecen flexibilidad a través de los modos de escaneo manual y programado
- Ofrecen enfoques estratificados para asegurar su computadora

6. ¿Cuáles son los beneficios de utilizar un cortafuegos (firewall) durante las teleconsultas?

Los cortafuegos protegen contra intrusos cibernéticos externos al proteger su computadora o red del tráfico de red malicioso o innecesario. Los cortafuegos también pueden evitar que el software malicioso acceda a una computadora o red a través de Internet. Se pueden configurar para bloquear datos de ciertas ubicaciones (por ejemplo, direcciones de redes informáticas), aplicaciones o puertos mientras permiten el paso de datos importantes y necesarios.

---

7. ¿Qué es el malware y cómo me deshago de él?

El malware es la abreviatura de *software malicioso:* software utilizado por piratas informáticos para dañar el funcionamiento de su dispositivo, robar datos o incluso tener el control de su propio dispositivo. Por lo general, el malware se descarga involuntariamente cuando un usuario desprevenido abre un archivo infectado o visita un sitio web infectado. Una vez que está en su computadora, lanza un tipo específico de ataque basado en su diseño. Por ejemplo, los keyloggers registran cada pulsación de tecla y comunican esta información a los piratas informáticos, que buscan nombres de usuario, contraseñas y otras credenciales confidenciales. Los troyanos se disfrazan de software útil o benigno, por ejemplo, software antivirus o juegos fraudulentos. Esto engaña a los usuarios para que le den paso al troyano, lo cual dará acceso a los archivos del sistema o facilitará la descarga de más malware.
Usted puede proteger su computadora contra el malware instalando un software antivirus y ejecutando el análisis de rutina. Si su computadora funciona lentamente o realiza acciones inusuales (como "recordarle" que descargue software extraño), es posible que esté infectada con malware. Ejecute un análisis con el antivirus para buscar, identificar y eliminar malware de su dispositivo.

---

8. ¿Por qué son importantes las contraseñas seguras y cómo crear una?

Es importante crear contraseñas seguras y únicas para todos sus inicios de sesión y cuentas en línea, no solo para las que usted utiliza en telesalud. Las contraseñas seguras son importantes para mantener sus cuentas en línea y su información personal a salvo de los ciberestafadores. Habilitar la autenticación con dos factores proporciona una capa adicional de seguridad.

Creación de una contraseña segura:

Paso 1: Utilice cinco palabras diferentes relacionadas con un recuerdo que sea único para usted. (por ejemplo, aprendiamanejarbicicletaalos5)

Cuanto más larga sea una contraseña, más difícil será adivinarla. Asegúrese de no utilizar información personal como su nombre, tarjeta de identidad de registro nacional (NRIC), fecha de nacimiento u otra información que pueda obtenerse fácilmente a través de una búsqueda en línea.
Paso 2: Utilice letras mayúsculas y minúsculas, números o símbolos para que sea aún más difícil de descifrar. (por ejemplo, AprendiaMANEJARbicicletaalos5)

Recuerde mantenerlo de manera aleatoria asegurándose de que su contraseña no tenga un patrón predecible, lo cual significa que otros no lo adivinarían fácilmente, incluso con herramientas especiales. Algunos ejemplos de patrones obvios incluyen:

- Utilizar frases comunes (p. ej., quelafuerzateacompañe)
- Escribir en mayúscula la primera letra de la contraseña (p. ej., Unavidalargaypróspera)
- Agregar un número al final (por ejemplo, qwerty1)
- Reemplazar una letra con un número o símbolo (por ejemplo, p@ssw0rd)

Ahora que creó con éxito una contraseña segura, habilite 2FA, lo cual significa una autenticación con dos factores, que agregará una capa adicional de seguridad a su cuenta.

9. ¿Cómo protege a mi computadora la actualización de mi navegador de Internet?

La actualización de su navegador de Internet proporciona una protección superior contra estafas, virus, troyanos, ataques de phishing y otras amenazas. También puede resolver las vulnerabilidades de seguridad presentes en su navegador actual. Se publican muchas actualizaciones del navegador para combatir estos problemas específicos. Para una seguridad y protección óptimas al utilizar Internet, ejecute siempre la última versión del navegador elegido que sea compatible con su sistema operativo.

11. ¿Qué estafas debo tener en cuenta?

No abra archivos adjuntos sospechosos ni haga clic en enlaces inusuales en los mensajes. Pueden aparecer en correos electrónicos, tweets, publicaciones, anuncios en línea, mensajes o archivos adjuntos. A veces también se disfrazan de fuentes conocidas y confiables.

Sepa cómo y cuándo lo contactaremos para su teleconsulta o para obtener cualquier información de seguimiento. Si recibe una llamada o correo electrónico sospechoso sobre su teleconsulta, comuníquese con su proveedor de atención médica. Más vale prevenir que lamentar.

12. ¿Qué es el phishing y cómo lo evito?

El phishing se refiere a cualquier tipo de comunicación digital o electrónica diseñada con fines maliciosos. Es un tipo de ataque de ingeniería social que utiliza la suplantación de identidad y el engaño, a menudo persuadiendo a una víctima inocente para que proporcione información confidencial, como credenciales de inicio de sesión, información de cuenta bancaria, número de seguro social u otros datos confidenciales.

El objetivo de un ciberestafador es utilizar esta información para estafar a la víctima de alguna manera: robar dinero, apoderarse de una o más cuentas, crear nuevas cuentas fraudulentas o aumentar los cargos de la tarjeta de crédito. En algunos casos, el objetivo final del intruso es apoderarse del dispositivo de la víctima utilizando software malicioso. El perpetrador también podría obtener acceso (a través de la víctima) a otros recursos valiosos, incluidas las redes, los sistemas, los datos o la propiedad intelectual de la empresa.

Recomendaciones para particulares:

- Tenga cuidado con todos los correos electrónicos y mensajes de texto no solicitados.
- Pase el cursor sobre los enlaces incrustados (sin hacer clic) para revelar la URL real y compararla con el enlace que se muestra.
- No haga clic en enlaces incrustados, incluso si cree que son confiables. Como alternativa, utilice su navegador para buscar la URL correcta.
- No abra archivos adjuntos de ningún tipo en correos electrónicos no solicitados. En el correo electrónico de remitentes conocidos, verifique los archivos adjuntos por separado antes de abrirlos.
- Comuníquese con su proveedor de atención médica acerca de correos electrónicos o mensajes de texto con enlaces incrustados o archivos adjuntos para validar esta información y asegurarse de que su privacidad esté protegida.
- Utilice antivirus y antimalware en sus dispositivos personales y manténgalos actualizados.
- Utilice la autenticación con varios factores en todas las cuentas que la ofrezcan, lo cual ayudará a evitar que los ciberestafadores accedan a sus cuentas.

13. ¿Cómo debo hacer una copia de seguridad de mis datos?

Puede realizar y almacenar copias de seguridad periódicas de toda la información valiosa en su dispositivo mediante el uso de medios externos o un servicio basado en la nube. El proceso se puede simplificar y automatizar mediante el uso de una aplicación de copia de seguridad de terceros. Asegúrese de cifrar su copia de seguridad para proteger la confidencialidad e integridad de su información. Las copias de seguridad de datos son importantes para minimizar los resultados negativos si los datos se pierden, dañan, infectan o roban.

14. ¿Qué elementos debo quitar antes de mi teleconsulta?

Antes de comenzar una conversación con su proveedor de atención médica, asegúrese de quitar los elementos que no sean necesarios para hablar sobre sus problemas de salud. Los dispositivos tecnológicos que no se utilicen para comunicarse con su proveedor de atención médica deberán retirarse para evitar capturar información potencialmente confidencial. Algunos ejemplos son las cámaras de seguridad del hogar o los asistentes de voz.