

# Consejos para profesionales de la salud: protección de datos en la telesalud



## ¿Qué riesgos hay en telesalud para la protección de datos y la seguridad?

- El riesgo para la protección de datos sucede cuando la persona no tiene control en la recopilación, el uso y la divulgación de su información médica.
- El riesgo para la seguridad sucede cuando ocurre un acceso no autorizado a la información médica de una persona durante su recopilación, transmisión o almacenamiento.
- Estos riesgos pueden afectar a la confianza entre el paciente y el profesional de la salud, y contribuir de manera negativa a la adhesión al tratamiento y a su continuidad.



## ¿Cómo cumplo con las obligaciones de protección de datos durante una teleconsulta?

- Los riesgos para la protección de datos y la seguridad existen tanto para las citas presenciales como para la monitorización a distancia y las teleconsultas. Las transmisión electrónica de datos implica mayor riesgo en la protección de datos y la seguridad.
- Asegúrese de estar al día sobre los requisitos de seguridad y protección para el [cumplimiento de la HIPAA](#) y de estar informado sobre otras [consideraciones legales](#).
- Los profesionales de la salud tienen la **obligación ética** de hablar con los pacientes sobre los riesgos para la protección de datos y la seguridad. Esas conversaciones pueden formar parte de un plan centrado en el paciente, para ayudar a garantizar la confidencialidad.



## ¿Cómo informo a los pacientes sobre la protección de datos?

- Confirme la identidad de todos los presentes en cada teleconsulta, y explique de qué forma podría estar involucrado algún tercero, para conseguir que la protección de datos sea parte del flujo de trabajo.
- Establezca las siguientes medidas preventivas e informe a los pacientes sobre ellas:
  - Genere N°s. de identificación de usuario exclusivos.
  - Utilice plataformas protegidas por contraseña
  - Configure el cierre de sesión como automático.



## ¿Cómo protejo mi propios datos y reduzco el riesgo de filtraciones?

- Las filtraciones de datos médicos son costosas y pueden suponer investigaciones, tener que notificar a los pacientes y recuperar los datos, de modo que los profesionales de la salud necesitan estar familiarizados con las herramientas de seguridad.
- Establezca los siguientes procesos:
  - Revise sus políticas de protección de datos y seguridad con regularidad.
  - Programe la eliminación periódica de los archivos en los dispositivos móviles.
  - Utilice procesos para hacer copias de seguridad de los datos y recuperarlos en caso de filtración.
- Haga que una entidad independiente lleve a cabo una **evaluación de seguridad** del sistema de telesalud, para verificar las funciones de seguridad como la autenticación, codificación, autorización y gestión de datos.
- Descubra más [consejos](#) de seguridad de la Oficina del Coordinador Nacional para Tecnologías de Información de Salud.