End-Stage Renal Disease Network Program

Seguridad en línea: Consejos para pacientes con ESRD

Sus proveedores de atención médica, sus planes de salud y otras organizaciones que trabajan con ellos deben cumplir las normas gubernamentales para mantener la privacidad de su información médica. Sin embargo, a medida que hay cada vez más formas disponibles de obtener y compartir información médica en línea, es importante que conozca los posibles riesgos de seguridad y tome medidas para proteger su privacidad.

¿QUÉ ACCIONES PODRÍAN PONERLO EN RIESGO?

- Realizar una encuesta en línea.
- Utilizar aplicaciones o dispositivos digitales para controlar su salud, como portales del paciente.

- Guardar su información médica en una aplicación o dispositivo móvil
- (teléfono inteligente, tableta).
- Compartir su información en redes sociales o en comunidades en línea relacionadas con la salud.

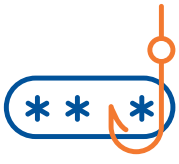
PROTEJA SU SEGURIDAD Y PRIVACIDAD

Contraseñas

- Utilice contraseñas seguras: Cree contraseñas que sean difíciles de adivinar.
- Mezcle letras, números y símbolos (al menos 14 caracteres).
- Actualice sus contraseñas con frecuencia.
- No comparta sus contraseñas con nadie

Correos electrónicos y mensajes

- ESPERE antes de responder cualquier correo electrónico o mensaje en el que se le pida información médica. Medicare y su centro NUNCA le pedirán información médica (o personal) por correo electrónico.
- NO responda correos electrónicos de personas que no conoce.



- NO haga clic en hipervínculos ni descargue archivos de fuentes desconocidas.
- Si el correo electrónico parece ser de una compañía que conoce pero no está seguro, compruebe con detenimiento que la dirección de correo electrónico del remitente y el contenido del mensaje no contengan faltas de ortografía. Aunque los correos electrónicos de algunos estafadores pueden parecer auténticos a primera vista, a menudo, cuando se miran con atención, se encuentran errores.

- NUNCA proporcione información médica a menos que esté seguro de que la solicitud es auténtica e informe los correos sospechosos a su proveedor de correo electrónico.
- Si no está seguro, pónganse en contacto con el remitente del correo electrónico directamente por teléfono o por mensaje de texto para verificar la comunicación.

continúa en la página siguiente

***Seguridad en línea** (continuada)*

Sitios web

- Asegúrese de que los sitios web que utiliza son seguros, especialmente si está ingresando información en el sitio. Busque que diga "https://" al comienzo de la dirección de un sitio web o ".gov" para Medicare u otros sitios relacionados con el gobierno.

Redes sociales

- Piense bien antes de publicar cualquier cosa en internet que no quiera que sea de público conocimiento; no dé por sentado que un foro público en línea es privado o seguro. Los estafadores pueden usar la información que publica.

- Si decide publicar información médica en una red social, considere la posibilidad de utilizar la configuración de privacidad para limitar el acceso de otras personas Tenga en cuenta que la información publicada en la web puede permanecer de forma permanente.

Teléfono

- NUNCA comparta su información personal o financiera por teléfono a menos que esté seguro de saber con quién está hablando.

- Si recibe una llamada sospechosa de alguien que le hace preguntas personales, cuelgue, busque el número de la organización y llámela directamente.
- Reduzca las comunicaciones no deseadas: Regístrese en la Comisión Federal del Comercio para que lo agreguen a la lista **NO LLAME**.

Precauciones generales de seguridad

- Confíe en sus instintos: Si tiene alguna pregunta sobre algo que pueda poner en riesgo la privacidad de su información médica, contáctese con su centro.
- Si está usando una red wifi pública, asegúrese de no utilizarla para comunicar información sensible sobre su salud o sus finanzas.

Si alguien llama para pedirle información o dinero
o para amenazar con cancelar sus beneficios de salud, cuelgue y llame al
1-800-MEDICARE (1-800-633-4227) • TTY: 1-877-486-2048

Para saber más sobre la tecnología de la información médica
sobre cómo mantener la privacidad y seguridad de su información, visite http://www.healthit.gov.

Fuente: The Office of the National Coordinator for Health Information Technology:
Health IT: How to Keep Your Health Information Private and Secure

End-Stage Renal Disease Network Program

Para presentar una queja, comuníquese con nosotros.

IPRO End-Stage Renal Disease Network Program
Corporate Office: 1979 Marcus Avenue, Lake Success, NY 11042-1072
Patient Services: (516) 231-9767 • Toll-Free: (800) 238-3773
Email: esrdnetworkprogram@ipro.org • Web: esrd.ipro.org

IPRO, la Organización para Enfermedades Renales Terminales de la Red de Nueva Inglaterra, Red de Nueva York, Red del Atlántico Sur y Red del Valle del Río Ohio preparó este material bajo contrato con los Centros de Servicios de Medicare y Medicaid (CMS), una agencia del Departamento de Salud y Servicios Humanos de los EE. UU. Número de contrato de CMS: 75FCMC19D0029 Números de órdenes de trabajo de CMS: 75FCMC21F0001 (Red 1), 75FCMC21F0002 (Red 2), 75FCMC21F0003 (Red 6), 75FCMC21F0004 (Red 9).
Publication # ESRD.IPRO-G2-20250130.430 2/10/2025 v.1 -vb