



Staying Safe Online: Tips for ESRD Patients

Your healthcare providers, health plans, and other organizations that work with them must follow government rules to keep your health information private. However, as more ways to get and share health information online become available, it is important for you to understand possible security risks and take steps to protect your privacy.



WHAT ACTIONS COULD PUT YOU AT RISK?

- Taking an online survey.
- Using digital apps or devices to monitor your health, such as patient portals.



- Storing your health information in a mobile application or on a mobile device (smartphone, tablet).
- Sharing your information on social media websites or health-related online communities.



PROTECT YOUR SAFETY AND PRIVACY

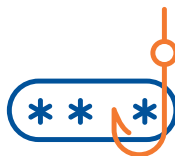
Passwords

- Use strong passwords: Create passwords that are hard to guess.
- Use a mix of letters, numbers, and symbols (at least **14** characters).
- Update your passwords often.
- Do not share your passwords with anyone.

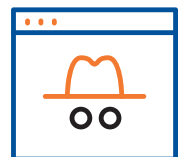


Emails and Messages

- **STOP** before you respond to any emails or messages asking for personal health information. Medicare and your facility will **NEVER** use email to ask you for personal (or personal health) information.



- **DO NOT** respond to emails from people you don't know.
- **DO NOT** click on links or download files from unknown sources.
- If the email looks like it's from a company you may know but you're not sure, carefully check the sender's email address and email content for misspellings. While some emails from scammers may look legitimate at first, oftentimes when you look closely, you'll find typos and other mistakes.
- **NEVER** provide personal information unless you're sure the request is legitimate, and report suspicious emails to your email provider.
- If you're unsure, contact the sender of the email directly by phone or text to verify the communication.



continues on next page

Websites

- Make sure that the websites you use are secure, especially if you are entering information into the site. Look for “https://” at the start of a website’s address or “.gov” at the end of the address for Medicare and other government-related sites.



Social Media

- Think carefully before you post anything on the Internet that you don’t want to be made public – do not assume that an online public forum is private or secure. Scammers can use the information you post.
- If you decide to post health information on a social media platform, consider using the privacy setting to limit others’ access. Be aware that information posted on the web may remain permanently.



Phone

- NEVER give your personal or financial information over the phone unless you are certain you know who you’re talking to.
- If you get a suspicious call from someone who is asking personal questions, hang up, look up the organization’s phone number, and call the organization directly.
- Reduce spam: Register with the **Federal Trade Commission** to be added to its national **DO NOT CALL LIST**.



General Safety Precautions

- Trust your instincts: If you have any questions about something that might put the privacy of your health information at risk, contact your facility.
- If you are using public wi-fi, be sure not to use it to communicate sensitive information about your health or your finances.



If someone calls asking for your information or money or threatens to cancel your health benefits, hang up and call 1-800-MEDICARE (1-800-633-4227) • TTY: 1-877-486-2048

To learn more about health information technology and keeping your health information private and secure, visit <http://www.healthit.gov>.

Source: 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

For more information or to file a grievance, please contact us:

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



This material was Developed by the IPRO ESRD Network Program, comprising the ESRD Networks of New York, New England, the South Atlantic and the Ohio River Valley, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. Views expressed in this material do not necessarily reflect the official views or policy of CMS or HHS, and any reference to a specific product or entity herein does not constitute endorsement of that product or entity by CMS or HHS. Publication # Publication # ESRD.IPRO-G3-NW-20220922-131 v.4 1/14/2024 vb

