HOW TO STAY IN THE
CYBER SAFETY ZONE

HOW YOU CAN PROTECT YOUR PATIENTS FROM THE TOP 5 CYBER THREATS

Social Engineering

Ransomware

Loss or Theft of Equipment or Data

Insider Accidental or Malicious Data Loss

Network Connected Medical Device Security

Social Engineering

- **Don't take the bait!**
- **Does the URL match the sender?** For example, if the sender is from Jackson Equipment, links should go to www.jacksonequip.com, not www.knjdlkajfkje.net.
- **Does the message elicit some type of quick action** such as "respond immediately" or "quick action is required?"

Ransomware

- **Utilize multi-factor authentication (MFA)** if your organization supports it. This will add another layer of protection for your data and systems.
- **Update your software and passwords** when your organization notifies you to do so.
- **Report anything suspicious.** It's always better to be safe and notify authorities immediately.

Loss or Theft of Equipment or Data

- **Know your organization's policy** regarding taking equipment home with you or from site to site.
- **Use a secure WiFi or VPN** whenever you are accessing organization data or sharing sensitive patient information.
- **Know your organization's encryption policies** when sharing data via email.

Insider Accidental or Malicious Data Loss

- **Follow your instinct,** and always report what does not look or feel right to you.
- **Beware of social engineering techniques like phishing**—these emails intentionally focus on human emotion, using words like, "Your immediate action is needed." Read thoroughly and proceed with caution.
- **Participate in all security awareness training** within your respective organizations to stay current with the latest threats and steps you can take to avoid them.

Network Connected Medical Device Security

- **Know your organization's protocols** for potential attacks on connected medical devices so you can react and act immediately.
- **Know your team.** Do you know who to contact if you suspect an issue with your network connected device?
- **Check the passwords.** Was the password changed on the connected medical device from the manuacturer or is it still an "admin" login and password? Default passwords should be changed immediately.

HHS 405(d)
Aligning Health Care Industry Security Approaches

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram!