Medical Practitioners

Cyber Care is Patient Care

You play a critical role in patient care and safety. And that role extends beyond the bedside in a hospital or the individual patient examining rooms at your medical office. Keeping you and ultimately your patients safe from cybersecurity threats is very important. Today, with the ever growing interconnectedness of our digital health environment in our facilities and network connected medical devices used by patients everyday, now is the time to review your "cyber chart" for important warning signs.

You triage patients everyday as part of patient care, but how good are you at triaging a cybersecurity issue when faced with one?

What are the cyber risks associated with the following questions:

- How many network connected medical devices do you use everyday? Is there a single "administrative" password associated with it?
- How many emails do you receive from unfamiliar sites asking you to take action by clicking on a link? What's the danger?
- Do you update your password when prompted by your organization? Why is this important?

These three circumstances provide opportunities for cyber attacks within your organization and network systems that manage patient care.

→ Any device connected to the network increases the chance of a cyber-attack.

→ Emails with links should be opened with caution! Know your sender before you click any links. Patient safety could be comprised with a breach caused by a phishing attack.

→ Always update your passwords when prompted to do so to keep your network safe and never share your passwords with anyone.

From securing network connected medical devices to password management, these are all critical care steps to keep you and your organization cybersafe! If any of these scenarios apply to you, contact your IT Administrator or Manager for further information regarding your specific unit/department.

Do you know the bedside connected medical device with the highest vulnerabilities?
#1 IV Pump [1]

Healthcare is more targeted for cyberattacks than any other industry, absorbing **100 to 200%** more attacks than the runner-up. [1]

Thanks to the volume of sensitive Protected Health Information (PHI), medical records can fetch up to **50 times** the amount that stolen credit cards get on the black market. [1]

1. Source: A Cynerio Report: The State of IoMT Device Security 2022

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 social media pages: **@ask405d** on **Facebook**, **Twitter**, **LinkedIn** and **Instagram**!