What you need to know about Ransomware:

Ransomware poses a threat to you and your device. What makes this form of malware so unique is the word "ransom". Ransomware is extortion software that can lock your computer and then demand a ransom for its release.

Cybersecurity threats to health care organizations and patient safety are real. Information technology, which provides critical life-saving functions, consists of connected and networked systems and leverages wireless technologies, leaving such systems more vulnerable to cyber-attack.

Steps to take

Review the list of best practices and follow each recommendation.

Action—Report

Contact your IT administrator, practice manager, or immediate supervisor. Any suspicious activity on your system? Add their name and number to this sheet for reference.

Quick action in this case is imperative. This threat is real!

Threat Quick Tips

HHS 405(d)
Knowledge on Demand

Most ransomware attacks are sent in phishing campaign emails. These messages ask you to either open an attachment or click on an embedded link.

- ☑ **Stay alert** when any email prompts you to enter your credentials.
- ☑ **Be cautious** before clicking any links in an email. Look at the sender address and hover over the URL.
- ☑ As a proactive measure, **check to see** whether the computer and network to which you are connected have the proper intrusion prevention system or software in place.
- ☑ Due to the severity and time sensitivity of ransomware attacks, **seek out professional IT security (or a similar point of contact)** help when you think your computer is infected with ransomware.

Reporting

Report to:

Contact Info:

For more resources and 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 (HICP)* publication at 405d.hhs.gov.