12 TIPS FOR SAFE TELEWORKING FROM HICP!

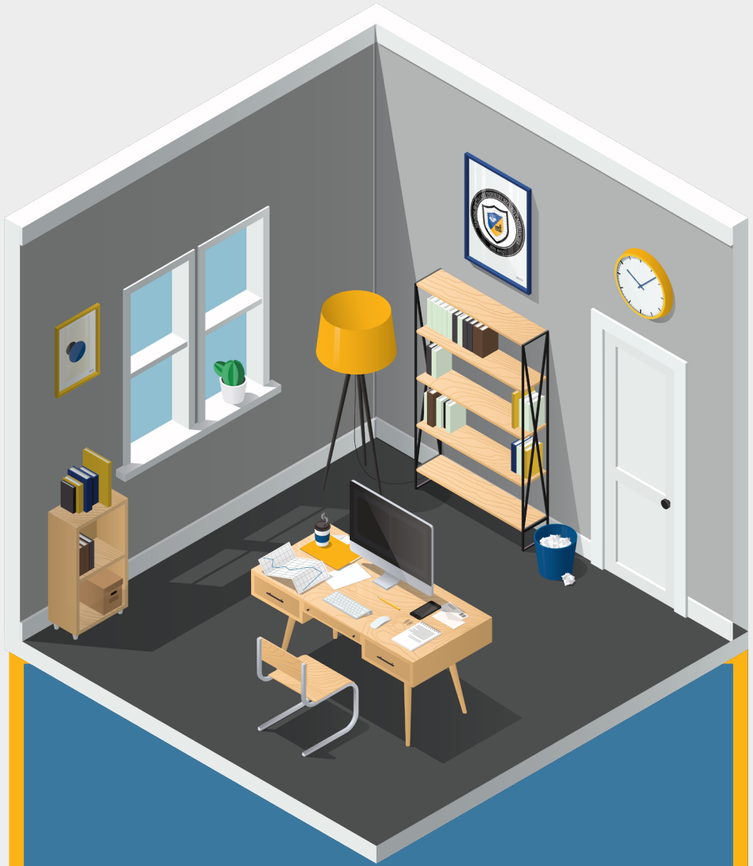
The healthcare workforce is always evolving and becoming more and more flexible. With this flexibility comes new risks and in order to continue to keep our patients safe from cyber threats we must practice vigilance while teleworking. The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication not only details how to protect healthcare organizations from cyber threats but also gives many tips on how to keep your teleworking space safe from cyber threats.

HHS 405(d)
Aligning Health Care Industry Security Approaches

*For more information on the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication to learn about telework mitigation practices check out our website at www.**405d.hhs.gov** or email us at cisa405d@hhs.gov*

WHAT YOU SHOULD DO AT WORK:

- Establish organizational policy and procedures for teleworking for your employees to follow
- Secure your teleworking equipment with the appropriate security scans and software
- Provide secure remote access such as a Virtual Private Network (VPN) for your employees
- Always keep device operating systems and apps up to date and available
- Provide training and awareness programs for your employees and explain the cybersecurity risks of teleworking
- Ensure policies and procedures are clear and distributed for reporting suspicious activity, potential, and actual breaches



WHAT YOU SHOULD DO AT HOME:

- Only access company data with your company equipment if possible
- Always use your company's secure remote access while working
- Protect your physical equipment by securing it in a secure location while away from the office
- Keep an eye out for social engineering and be vigilant in recognizing email phishing scams
- While teleworking avoid using open public internet networks, always ensure you have a private network
- Stay alert and report suspicious activity to the appropriate department immediately