Equipment

Many cybercriminals gain access to healthcare organizations through stolen or lost laptops, phones, tablets and other equipment. Always encrypt sensitive data on your devices and immediately report to your IT department if your equipment is missing!

Passwords

Passwords are the gateway to your organization's network and connectivity. Use strong passwords for your work and personal accounts and change default passwords for equipment and network access to keep your patients safe. Always use different passwords that don't contain personal identifiers.

KEEP A BALANCED CYBERSECURITY DIET!

Just as it is important to have a balanced diet it is also important to have a balanced cybersecurity approach in order to protect your patients from all cyber-threats.

Have questions? Checkout HICP!

Most Ransomware attacks begin with Email Phishing, therefore, always remember to double check the sender of an email and check hyperlinks by hovering your mouse over them to show the web address prior to clicking.

Email Protection

Cyber-attacks on healthcare organization's networks cause serious impact to patient care. Always ensure you are using your organization's Virtual Private Network (VPN) when accessing patient data from home or at the office!

Network Protection

HHS 405(d)
Aligning Health Care Industry Security Approaches

For more information on how to keep a balanced cyber diet check out our website at 405d.hhs.gov. There you'll find the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication to learn about the top 5 threats facing the healthcare industry and ten practices to mitigate them!