Practice Administrators & IT Professionals

Cyber Care is TOTAL Care

These functions and/or roles in healthcare organizations play a critical role in keeping patients, visitors and hospital networks safe from cybersecurity threats.

Provider practice management includes patient access and registration, patient accounting, patient scheduling, claims management, and bill processing.

Business operations includes accounts payable, supply chain, human resources, IT, staff education, protecting patient information, and business continuity/disaster recovery.

Health-IT is a critical component of almost every healthcare organization. Electronic health records (EHRs), medical devices, and business management software applications have been integrated into clinical practice and health care operations.

Cybersecurity Best Practices to protect patient data:

From securing network connected medical devices to password management, these are all critical care steps to keep your patients' healthcare records cybersafe!

Password Protection	Update your password regularly, and immediately upon learning of a breach that may have compromised the passwords.
MFA (Multi Factor Authentication)	Implement MFA to provide a second layer of security for your data and applications.
Encryption	Install encryption software on every endpoint.
Software Updates	Ensure software programs are updated to maintain security updates.

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**!