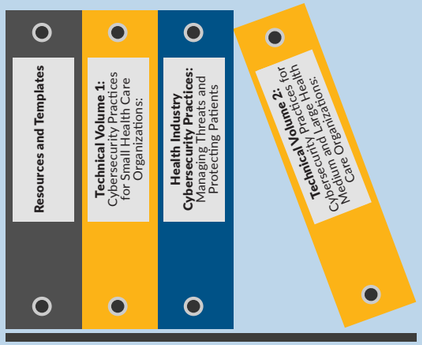
IS YOUR ENTERPRISE EVOLVING TO PROTECT PATIENTS?

Before health records became digital, the healthcare industry went through great lengths to provide safe storage and transfer of patient's PHI. Locked warehouses were built and credentials were required in order to transfer PHI files to other offices.

With the cyber threat landscape expanding every day, staying up-to-date on cybersecurity practices can seem difficult and overwhelming. Now more than ever, it is crucial for us to evolve our security mechanisms to continue to protect patients in the digital age.

This is where the health sector public private partnership comes in. The Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication is a free resource that can get you started in your cybersecurity journey.



The ten practices listed below from the five threats within the HICP publication are designed to help keep your patients safe from various types of cyber threats. Check out the HICP Publication to learn more about how to implement these mitigation practices in your organization!

- E-mail protection systems
- Endpoint protection systems
- Access management
- Data protection and loss prevention
- Asset management
- Network management
- Vulnerability management
- Incident response
- Medical device security
- Cybersecurity policies

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 and check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov or our Social Media pages @ask405d on Facebook, Twitter, and Instagram!