HHS 405(d) PROGRAM

Aligning Health Care Industry Security Approaches

Current State in Healthcare and Public Health (HPH) Sector

On average, every employee has access to over

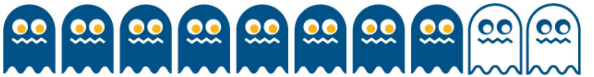
11 million

files, nearly **20%** of the organization's total files.

On average, more than

1 in 10

sensitive files are open to every employee.



79% of organizations have **more than 1,000 ghost users** still enabled.

OVER 50% Over 50% of organizations have **more than 1,000 files** open to every employee.

ABOUT 2/3 About two-thirds of organizations have **500+** accounts with passwords that **never** expire.

On their first day, new employees at small companies have instant access to

over 11,000

exposed files and **nearly half** of them contain sensitive data.

Organizations that willfully neglect HIPAA Rules and make no effort to protect sensitive patient data could be fined **up to**

$1.5 million

per year.

$7.13 MILLION The average cost of a data breach in the healthcare sector was **$7.13 million** in 2020.

Ransomware in 2020

In 2020, the number of **ransomware attempts** against the healthcare industry rose by

123%

- 2021 SonicWall Cyber Threat Reportt

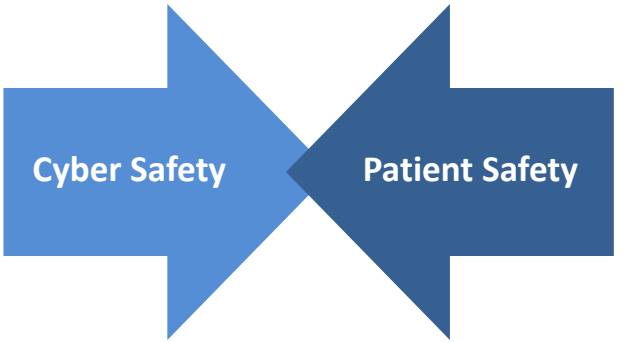
Ransomware attacks cost the healthcare industry

$20.8 billion in downtime

in 2020, which is double the number from 2019.

- Comparitech Annual Report

Cyber Safety is Patient Safety



Cyber attacks in healthcare affect every aspect of an organization, but, most importantly they affect **patient safety.**

A single cyber attack has the potential to shut down care facilities, erase important patient health history, and put your patient's health and identity at risk.

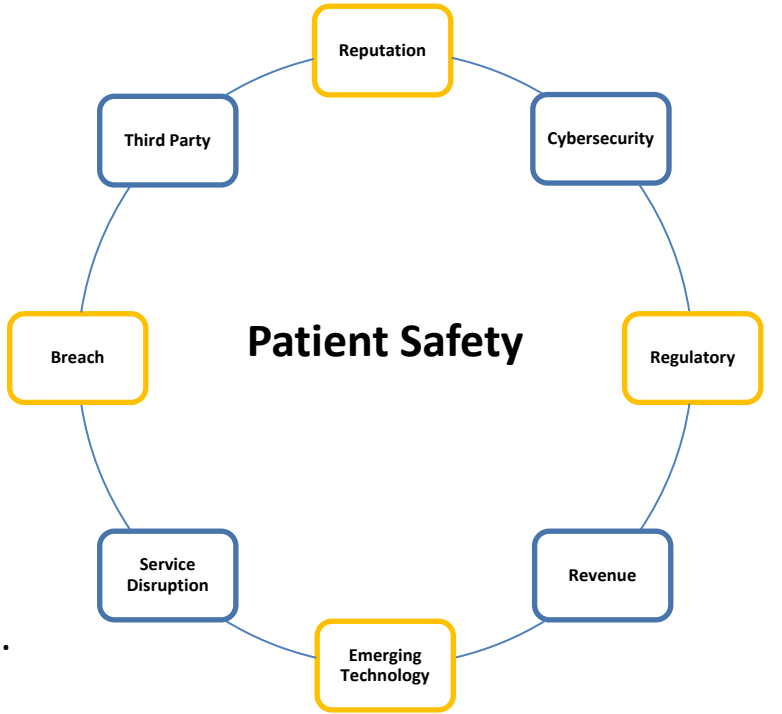
Enterprise Risk Management and the Inclusion of Cyber

ERM is an effective organization-wide approach to addressing the full spectrum of the organization's significant risks by **considering the combined array of risks as an interrelated portfolio**, rather than addressing risks only within siloes.

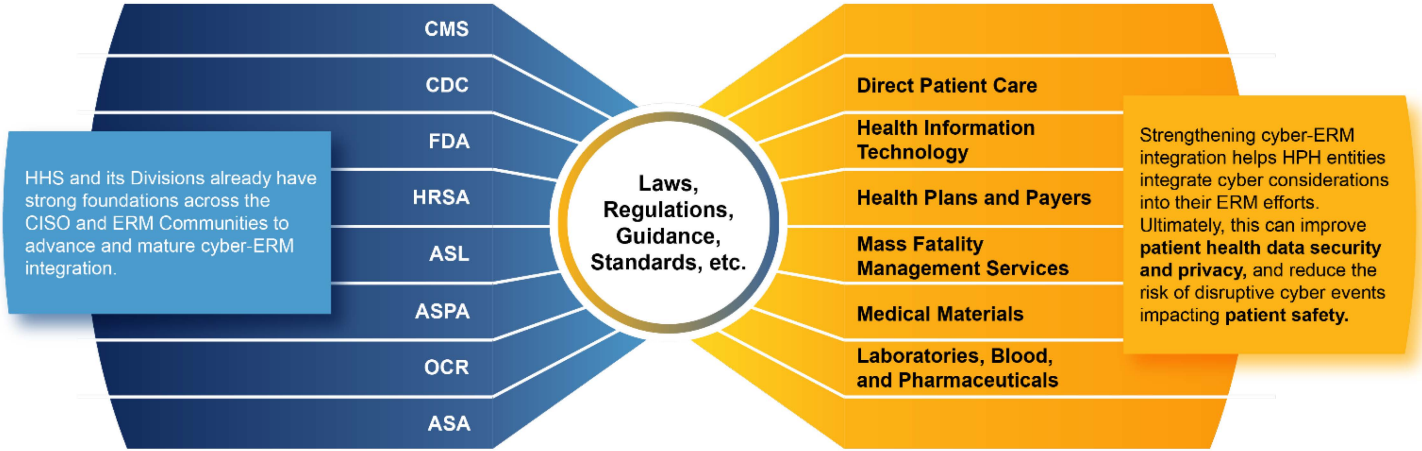
- Risks are interrelated
- ERM helps tie these into mission impacts
- ERM supports credible decision-making based on risk and opportunity information
- ERM normalizes risks across many domains to allow comparability

Cybersecurity risks are **one** of **many** enterprise risks.

These risks can affect every aspect of a healthcare organization including its reputation**.** The most important risk is to **patient safety,** which is the corner stone of every health organization.



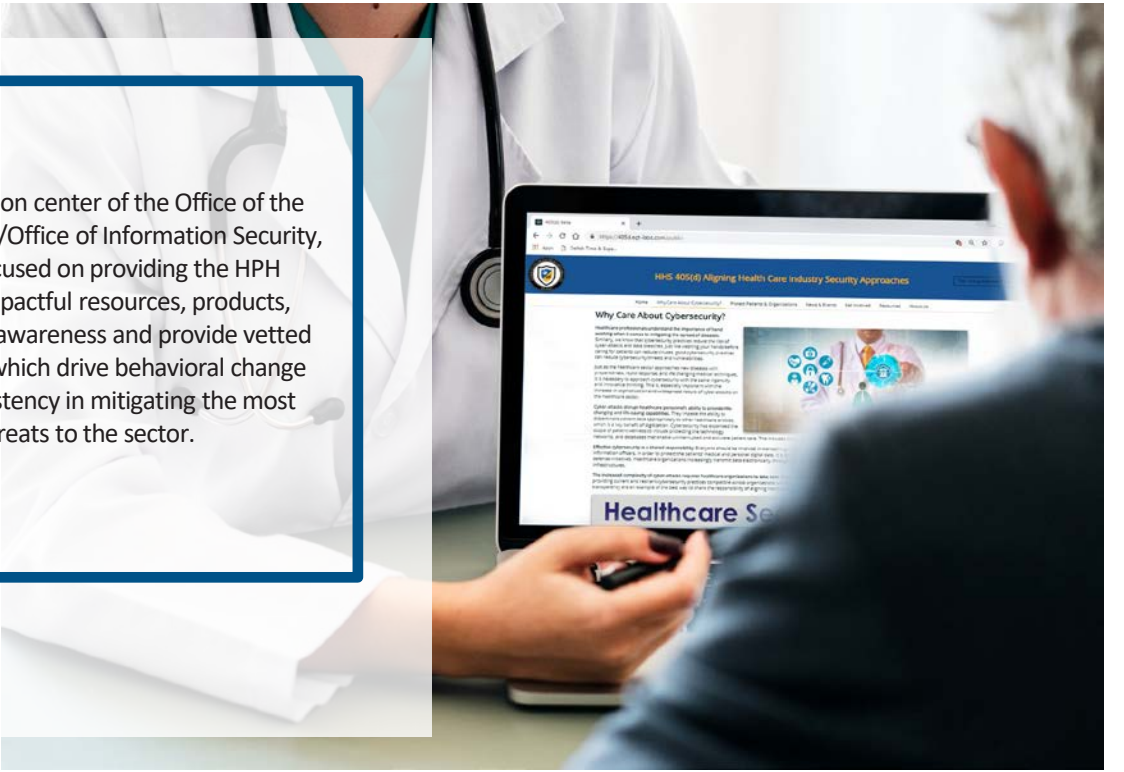
HHS ERM Impact on the HPH Sector



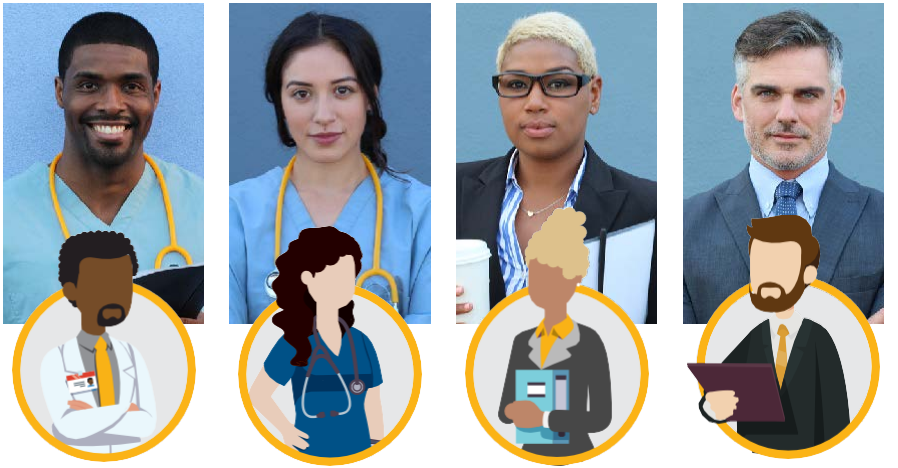
Aligning Healthcare Industry Security Approaches

Mission

As the leading collaboration center of the Office of the Chief Information Officer/Office of Information Security, the 405(d) program is focused on providing the HPH sector with useful and impactful resources, products, and tools that help raise awareness and provide vetted cybersecurity practices, which drive behavioral change and move towards consistency in mitigating the most relevant cybersecurity threats to the sector.



405(d) Task Group



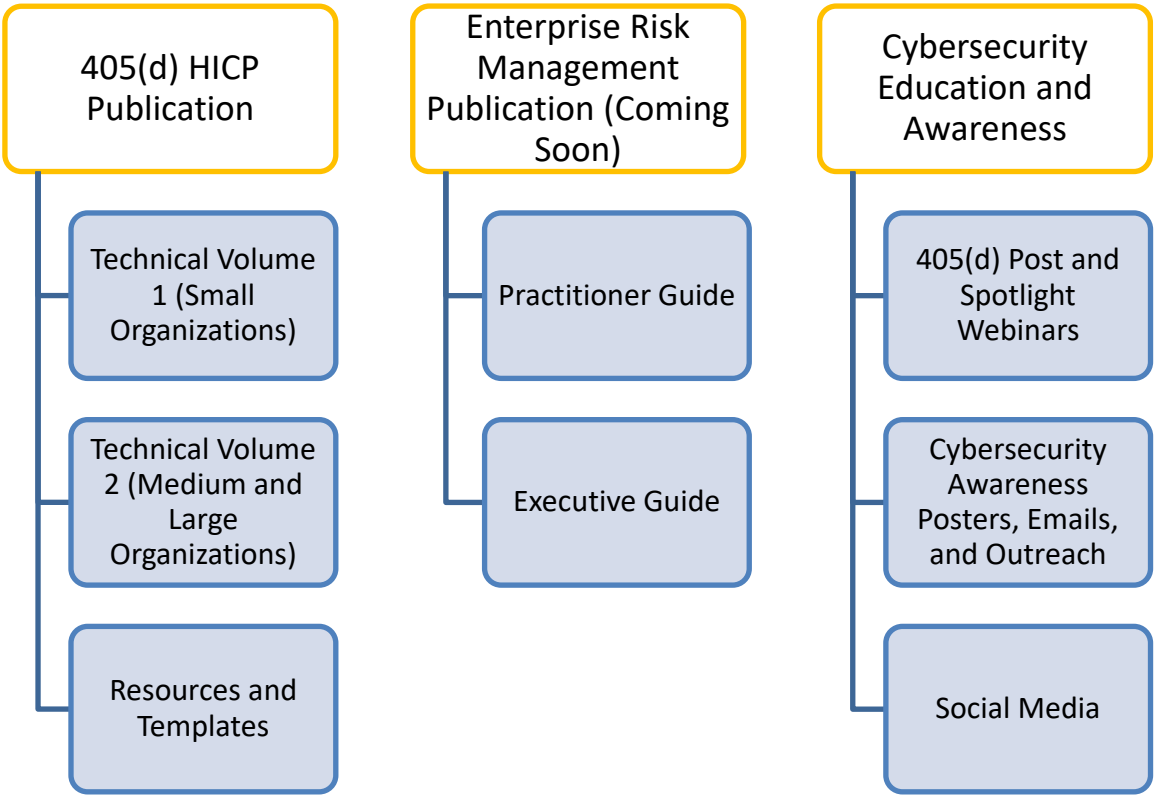
The core of the 405(d) program is it's task group members. Convened by HHS in 2017, the 405(d) task group is comprised of over **230 +** information security officers, medical professionals, privacy experts, and industry leaders.

The task group members help drive all aspects of the 405(d) program, to include official program products, awareness campaigns, engagements, and outreach channels.

The task group is actively collaborating and working on a host of new resources for the sector including an update to the HICP publication and a new ERM Cybersecurity publication both of which are planned to be released in 2021/early 2022

405(d) Products to support ERM in the HPH sector

Cybersecurity risks are enterprise risks that can affect every aspect of an organization including reputation. The most important risk is **patient safety,** which is the corner stone of every organization.



Questions?

Do you follow us on Social Media?
Check us out at **@ask405d**

Linkedin.com/company/hhs-ask405d