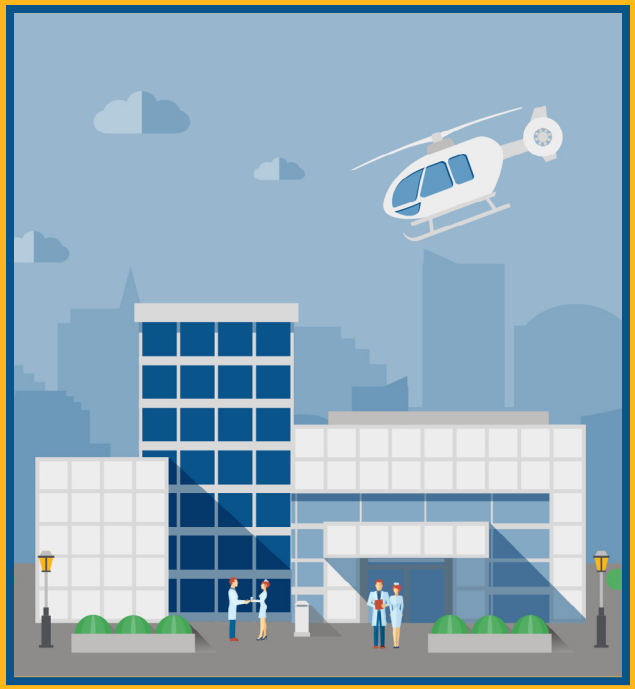
# Looking for Practical Solutions for Addressing Cybersecurity Risks?

The Health Industry Cybersecurity Practices (HICP) is a free publication produced by the public/private partnership between the U.S. Department of Health and Human Services (HHS) and the Health & Public Health Sector Coordinating Council.

The 405(d) Task Group has created Quick Start Guides to help guide you through HICP, and to ensure proper assignment of your resources in order to reduce and mitigate threats to your healthcare organization. Click HERE to access the **Quick Start Guide for Medium to Large Organizations.**



**HHS 405(d)**
Aligning Health Care Industry Security Approaches

Health & Public Health Sector Coordinating Council
**PUBLIC PRIVATE PARTNERSHIP**

**Want more information or need to obtain a copy of the HICP Publication?** Please visit the 405(d) website at 405d.hhs.gov or email us at CISA405d@hhs.gov.

## Cybersecurity is a Business and Patient Safety Risk:

# Are you adequately addressing cyber?

Cybersecurity is in the news, but knee jerk reactions based on the latest phishing, ransomware, or other threats are not effective. Cybersecurity risk is not just an IT risk; it's a business risk that needs to be addressed accordingly.

Hackers of all types (i.e. organized cyber crime, insiders or those familiar with your practice) make money from illegally obtained and ransomed healthcare data from your healthcare organization and vendors. Business risks from cybersecurity threats run the gamut from reputation to financial and even regulatory impact, which is why hospitals and healthcare systems must mitigate cybersecurity threats.

## 40 million patients

In 2020, health record breaches exceeded **40 million patients.**

## 905 breaches reported

**905 breaches** were reported to HHS in 2021.

## 83%

Percentage of organizations that have had **more than one breach**

Healthcare breach costs have been the **most expensive industry for 12 years running, increasing by 41.6%** since the 2020 report.

Healthcare is one of the more **highly regulated industries** and is considered **critical infrastructure** by the US government.

## 19%

Frequency of breaches caused by stolen or compromised credentials

## $4.35 million

In 2022, data breach costs rose **2.6%** from the previous year coming in at a cost of **$4.35 million dollars.**

## $1.51 million

Average breach cost savings associated with a mature zero trust deployment versus early adoption of zero trust.

Data from 2022 IBM Cost of a Data Breach Report.

Visit our website at 405d.hhs.gov and follow us on social media! @ask405d