Looking for Practical Solutions for Addressing Cybersecurity Risks?

The Health Industry Cybersecurity Practices (HICP) is a 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.

We know you're busy. That is why HICP was designed with you in mind. It has a special section for small healthcare practices with practical, low-cost solutions that you can put in place TODAY.

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 Small 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:

Do you treat patient data with the same level of care as your patients?

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 a technology risk; it's also a risk to your patients and your business 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. Business risks from cybersecurity threats run the gamut from reputational to financial to workflow, which is why small healthcare organizations must mitigate cybersecurity threats.

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.

A majority of organizations in the study said they **increased the price of their products and services** as a result of the data breach.

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

19%

The most common initial attack vector in 2022 was **stolen or compromised credentials,** responsible for **19%** of breaches in the study.

Data from 2022 IBM Cost of a Data Breach Report.