What's New in the HICP 2023 Edition

HHS 405(d)
Aligning Health Care
Industry Security Approaches

What is Health Industry Cybersecurity Practices (HICP) and why is it important?

HICP aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid Healthcare and Public Health organizations to develop meaningful cybersecurity objectives and outcomes. The publication outlines the top 5 threats facing the healthcare sector and the ten mitigating practices to combat them. The HICP 2023 Edition includes:

- **Main Document**—Provides an overview of the 5 threats facing the Healthcare sector and instructions on how to use this publication.
- **Technical Volume 1**—Provides the 10 cybersecurity practices and many sub-practices for small entities that can be implemented to combat the 5 threats.
- **Technical Volume 2**—Provides the 10 cybersecurity practices and many sub-practices for medium and large entities that can be implemented to combat the 5 threats.

Not new to HICP? Here's why you should read the 2023 Edition:

Cybersecurity threats evolve each year and with them comes new mitigating practices. The HICP 2023 Edition has been updated by industry and government professionals to include the most relevant and cost-effective ways to mitigate the current cybersecurity threats the HPH sector is facing. This edition of HICP includes a new top 5 threat and many new mitigating practices that you should be implementing in your organization to continue to keep patients safe. Cybersecurity requires us to be flexible and preemptive. This new edition addresses cybersecurity trends the HPH sector is seeing and it will help your goals to uphold patient safety in your organization.

HICP Main Document includes new cybersecurity strategies

The HICP Main Document has been updated to renew our call to action to maintain patient safety and includes new cybersecurity strategies such as **Zero Trust** and **Defense in Depth**. It also now includes a section on the importance of workplace training and awareness and provides guidance on why each role in a HPH organization is important to keep patients safe from cyber threats.

UPDATED THREATS

The threat Email Phishing is now labeled as Social Engineering

While the definitions between both editions are similar, social engineering threats encompass more than just email phishing. Some new items addressed by this new threat: Smishing, Whaling, Business Email Compromise, and more!

UPDATED PRACTICES

Cybersecurity Practice #9 on Network Connected Medical Devices has been fully updated

This section has been thoroughly updated with new sub-practices to ensure the protection of the growing use of network connected medical devices in the HPH sector.

Cybersecurity Practice #10 has been updated from Cybersecurity Policies to Cybersecurity Oversight and Governance

In addition to policies, this section includes governance and oversight structures each organization should have in place for an effective cybersecurity program.

NEW SUB-PRACTICES

New Sub-practices that have been added include:

- **Attack Simulations (Practice #7):** This section provides entities a guide on the importance of performing attack simulations and outlines what to include in your own simulations.
- **Cybersecurity Insurance (Practice #10):** This section provides entities new information on why cyber insurance is important and what your cybersecurity insurance policies should cover.
- **Cybersecurity Risk Assessment and Management (Practice #10):** This section provides entities on how to perform risk assessments and even provides free federal tools you can utilize to perform your own Risk Assessment.

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Healthcare & Public Health Sector Coordinating Counc PUBLIC PRIVATE PARTNERSHIP

Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

Healthcare & Public Health Sector Coordinating Counci PUBLIC PRIVATE PARTNERSHIP

Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations

Healthcare & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP

UPDATED THREATS AND PRACTICES

Top 5 Threats

1. Social Engineering
2. Ransomware
3. Loss or Theft of Equipment or Data
4. Insider Accidental or Malicious Data Loss
5. Attacks Against Network Connected Medical Devices

Ten Practices

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Network Connected Medical Device Security
10. Cybersecurity Oversight and Governance

While those listed above are the major updates, please note each of the 10 practices listed has been reviewed and updated to ensure the most up-to-date cybersecurity mitigations are provided and can be put in place today by organizations of all sizes. We encourage everyone, including those who are familiar with HICP, to read the new 2023 Edition to ensure your organization is incorporating industry-tested best practices that can fight the cyber threats of today.

To read the full publication, visit our website at 405d.hhs.gov.