

No Excuses | We have FREE Cybersecurity Resources!

HHS 405(d) provides significant free resources and guidance designed to help you protect your business and your patients

Presenter: Karen Blanchette, MBA

Professional Association of Health Care Office Management | PAHCOM



**Ambassador for
HHS 405(d)**

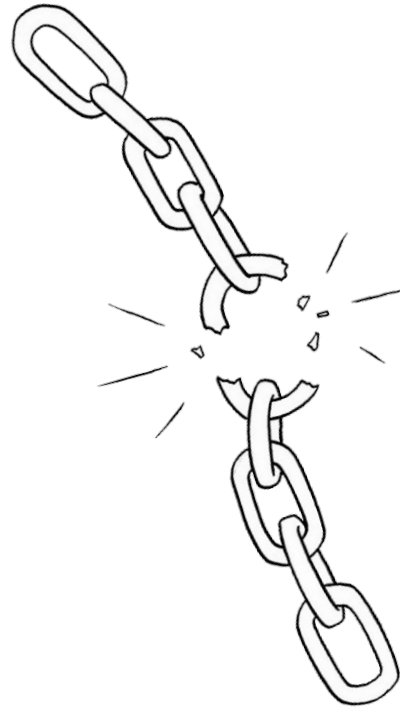
**Aligning Health Care
Industry Security Approaches**

This presentation is accurate to the best of my knowledge as of this date but is also condensed and paraphrased to fit the time allotted.

This information is not legal or business advice. It is intended to offer direction and navigation of free resources from HHS.

While the bulk of information presented is public domain, the presentation itself is the sole property of PAHCOM. It may be shared in its entirety in the context of today's event only.

Everyone who logs into any device at the practice needs to be cyber-aware!



The IT Guy, if you have one, might be the person you direct questions to. But every user on a network must be aware of basic threats and know what to do when they see one. The “weakest link” concept applies and each user is a link.

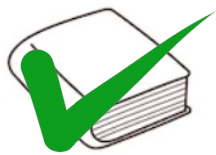
HHS 405(d) Aligning Health Care Industry Security Approaches

<https://405d.hhs.gov>

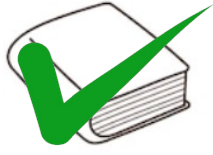


As a result of the Cybersecurity Act of 2015, the U.S. Department of Health and Human Services brought together over 150 cyber-experts, clinicians and healthcare administrators to develop the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

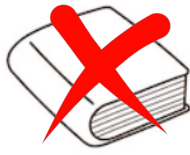
Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)



Main Document

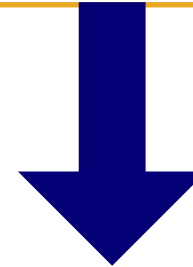


Technical Volume 1



Technical Volume 2

Use the HICP Quick Start Guide!



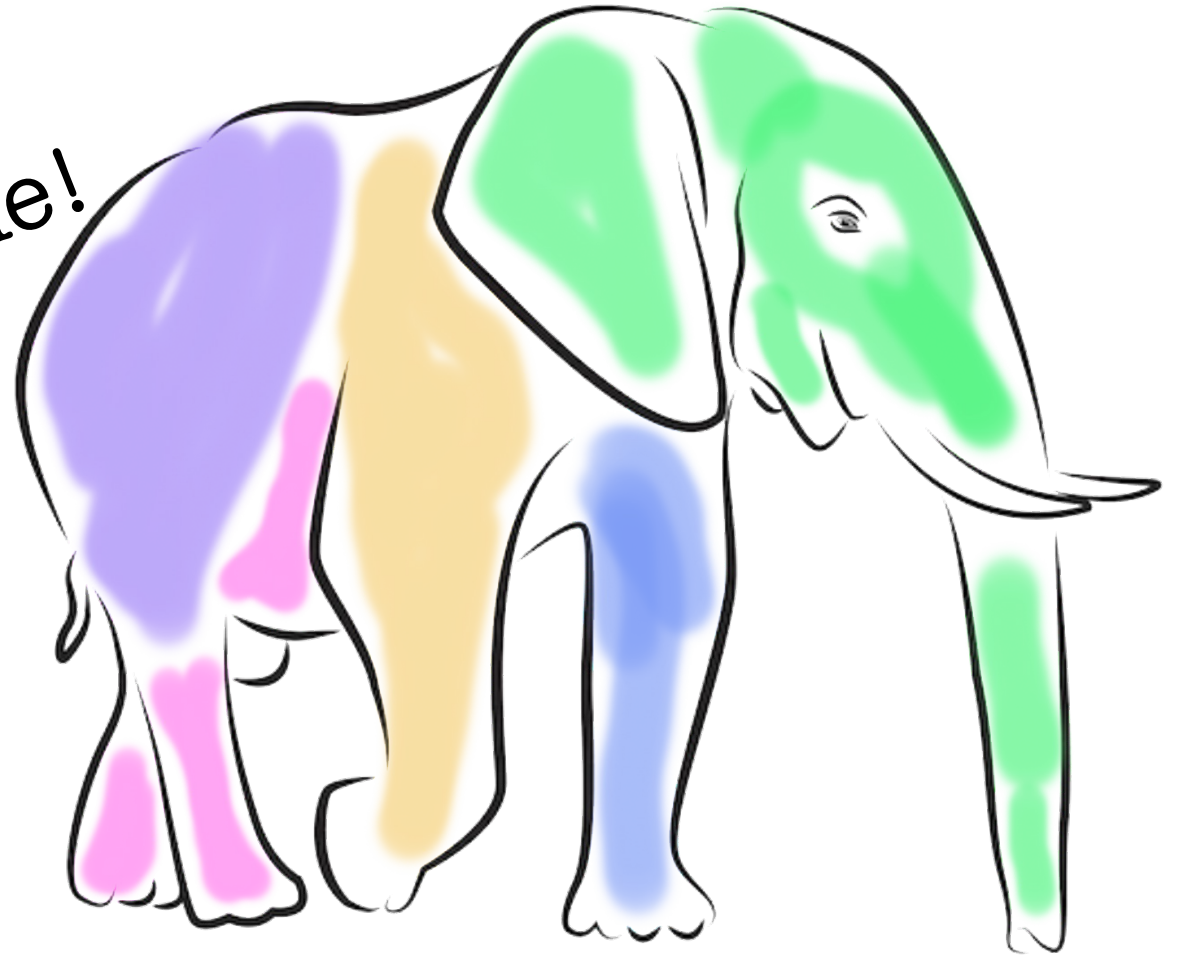
Leadership & Management

MD – pages 5-10
MD – page 28
T1 – pages 3-4

Five of the Most Current and Common Cybersecurity Threats

*One bite
at a time!*

1. E-mail phishing
2. Ransomware
3. Loss or theft of equipment or data
4. Insider, accidental or intentional data loss
5. Attacks against connected medical devices that may affect patient safety

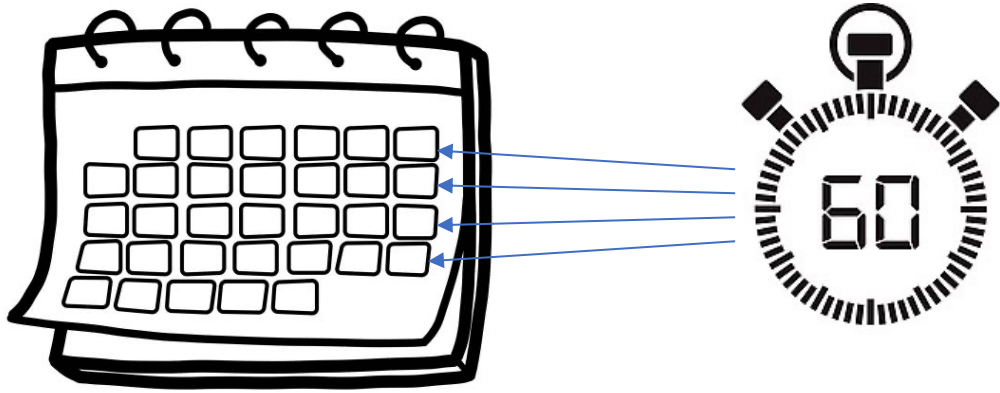


PUBLIC LAW 116-321—JAN. 5, 2021



This law amends the HITECH Act allowing special leniency for covered entities and business associates who tried to do the right thing by following 405(d) guidelines and best practices (over the past 12 months). It might not prevent all attacks, but now you get credit for a year of due diligence!

Take ACTION Now!



Use the free HHS 405(d) resources. This link provides materials for weeks 1-4 to help you get started.
<https://my.pahcom.com/405d>

Consider a one hour/week plan. Begin with an overview then dive into the 5 threats.

Week 1



Week 2



Week 3



Week 4



thank you

Slides and links to information referenced here are available FREE to the public at <https://my.pahcom.com/405d>



<https://my.pahcom.com/405d>

Karen Blanchette, MBA
Executive Director | PAHCOM
Ambassador for HHS 405(d)
karen@pahcom.com

