



HHS 405(d)

Aligning Health Care
Industry Security Approaches



Healthcare & Public Health
Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

405(d) Spotlight Webinar Series

Message from the 405(d) Team

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication and this engagement, are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC).



Healthcare & Public Health
Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) task group member each iteration and do not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute this webinar series.



405(d) Events and Announcements

➤ December

- Happy Birthday HICP! December 28th
- HC3 Private Sector Briefing: Supply Chain Risk Management- December 19th at 1pm EST – Email at HC3@hhs.gov

Email Us!

CISA405d@hhs.gov

➤ January

- 405(d) and North Carolina Health and Human Services Cybersecurity Town Hall (1/22)

➤ February

- Spotlight Webinar Featuring Greater New York Hospital Association: Date TBD

Upcoming
EVENTS



Agenda

Time	Topic	Speaker
<i>5 minutes</i>	Opening Remarks and Introductions	Julie Chua
<i>10 minutes</i>	Ransomware Overview	Julie Chua
<i>20 minutes</i>	HC3 Ransomware Threats	Greg Singleton
<i>15 Minutes</i>	Ransomware Resources	DHS- Kirsten Duncan, Kevin Dillon; H-ISAC-Errol Weiss; HHS-Julie Chua
<i>5 Minutes</i>	Q&A	All
<i>5 minutes</i>	405(d) Closing	405(d) Team



Presenters

Julie Chua

*Director, Governance, Risk, and Compliance
HHS Cybersecurity Program Office of Information
Security
U.S. Department of Health and Human Services*

Greg Singleton

*Director, Health Sector Cybersecurity Coordination
Center (HC3)
U.S. Department of Health and Human Services*

Kirsten Duncan

*Cybersecurity Division
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security*

Kevin Dillon

*Stakeholder Engagement Division
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security*

Errol Weiss

*Chief Security Officer
Health-ISAC (Health Information Sharing and Analysis
Center)*



Cybersecurity Act of 2015 (CSA): Legislative Basis

Under the auspices of the Cybersecurity Act of 2015 (CSA), Section 405(d), the U.S. Department of Health and Human Services (HHS) convened the CSA 405(d) public/private task group to enhance cybersecurity and align industry security practices.

The purpose of the 405(d) Spotlight Webinar is to continue the 405(d) mission and vision of “Aligning Health Industry Security Approaches” by discussing a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations.

This webinar series aims to align industry security practices by providing an information sharing platform for our public/private partnership. For more information on the 405(d) Program please email us at CISA405d@hhs.gov !

CSA Section 405

Improving Cybersecurity in the Healthcare Industry

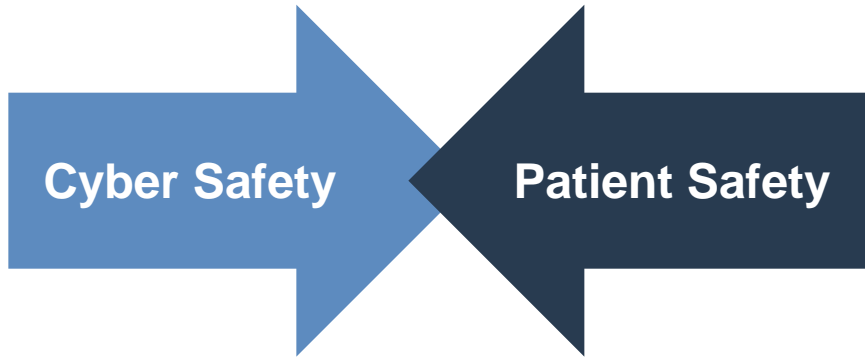
Section 405(b):
Healthcare Industry
Preparedness
Report

Section 405(c):
Healthcare Industry
Cybersecurity Task
Force

Section 405(d):
Aligning
Healthcare
Industry Security
Approaches



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.





HHS 405(d)

Aligning Health Care
Industry Security Approaches



Healthcare & Public Health
Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

Ransomware

Ransomware

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.

However, **paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data.**

Ransomware threats may incorporate tactics or techniques that are the same as or identical to other threats.



Cybersecurity Impact on the Healthcare Industry

In the Headlines...

“Three Hospitals in Alabama Divert Patients Due to Ransomware attack”

“Ransomware Hits 400 Dental Offices Across the US”

“Medical Practice to close in Wake of Ransomware Attack”

“Ransomware Attack Shuts Down Local Medical Practice- All Records Lost”



18%

percent increase in ransomware attacks on the Health Sector in 2019 compared to 2018

Healthcare ransomware attacks will increase

x4 by 2020





HHS 405(d)

Aligning Health Care
Industry Security Approaches



Healthcare & Public Health
Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

Ransomware in the HPH Sector HC3

Ransomware vs. Healthcare Industry

▶ Ransomware is frequently used to target healthcare:

- Cylance Threat Report (May, 2018)
 - Ransomware attacks tripled in 2017
 - Healthcare was targeted more than any other industry
- Solutionary Security Engineering Research Team (Q2, 2016)
 - 88% of all ransomware attacks target the healthcare industry
- Herjavec Group 2017 Healthcare Cybersecurity Report
 - Ransomware attacks on the healthcare sector will quadruple by 2020
- Kaspersky Cyber Pulse: The State of Cybersecurity in Healthcare (December, 2018)
 - 2018: One in four healthcare organizations successfully attacked by ransomware
- McAfee Labs Threats Report: August 2019
 - 504 new threats per minute in Q1 2019; New ransomware up 118%
 - ~50% of all ransomware attacks in the last year targeted North America

▶ Ransomware can cripple a healthcare provider, bringing operations to a halt

- Sept 20th – A hospital in Wyoming shut down some operations, postponed surgeries, diverted patients due to a ransomware attack.
- As of this year, research indicates that there have been hospitals and direct patient care facilities that have closed permanently after being victims of ransomware attacks.

Ransomware attacks more rampant than many hospitals might think, Kaspersky says

New research showed that organizations don't always learn their lesson the first time around, with 33 percent of survey respondents saying ransomware attacks happened more than once.

By [Beth Jones Sanborn](#) | December 18, 2018

Healthcare IT News



Threats on our Radar: Ryuk

▶ Why the name “Ryuk”?

- Fictional character in Japanese comic book series entitled Death Note
 - Shinigami (God of Death) – who invites human beings to death by dropping notes

▶ Ryuk Ransomware

- First identified in 2018
- Initially thought to be Hermes
- Likely utilized by Russian criminal groups
- Deliberately used against relatively big targets
- Typically, 15 – 50 bitcoin (BTC) each (1 BTC = ~\$8,723 as of November 2019)
- \$3.7M in BTC so far across 52 transactions
- Used by various APTs and criminal group threat actors such as:
 - Grim Spider
 - TEMP.Mixmaster

Source: <https://www.coindesk.com/price/bitcoin>



MalwareHunterTeam
@malwrhunterteam

Follow

From 13th this month, we seen 5 victims of a ransomware. At least 3 of them are companies (from those, 2 are from US, 1 from Germany, and 1 of the 3 is healthcare related).

The ransom note seems Bitpaymer, encrypted files seems Hermes. Strange.



[@BleepinComputer](#) [@demonslay335](#)

12:00 PM - 17 Aug 2018

19 Retweets 23 Likes



2



19



23



Threats on our Radar: Sodinokibi

▶ Historical Aspect:

- First discovered by Cisco Talos research conducted in April 2019 by researchers
- Also known as REvil and Sodin

▶ Key Identifiers and things to know about Sodinokibi:

- Strain of ransomware that has similarities with GandCrab; possibly same operators
- Utilized by GOLD SOUTHFIELD threat group (Secureworks)
- Named “The Crown Prince of Ransomware”
- Does not impact Commonwealth of Independent States (CIS) or Syria
- Upgraded versions of Sodinokibi have already been released in the wild
- New TTP – compromising MSP
- Ransoms observed within Sodinokibi attacks: \$1,500 - \$2,500 in Bitcoin per instance

▶ Technical capabilities of Sodinokibi:

- Encrypt non-whitelisted files/folders on local storage devices and network shares
- Terminate blacklisted processes prior to encryption to eliminate resource conflicts
- Wipe the contents of blacklisted folders
- Can perform exfiltration on basic host information



COMMONWEALTH OF INDEPENDENT STATES



Sodinokibi: How does a Managed Service Provider (MSP) attack occur?

- ▶ Ransomware attack on Managed Service Provider (MSP) serves as mass attack vector
 - Step 1: Managed Service Provider is compromised by attackers and ransomware is inserted in communications pipe with clients
 - Step 2: Managed Service Provider transmits and receives data with clients, including ransomware
 - Step 3: Ransomware compromises clients; Their files are inaccessible



THREAT ACTOR

How to Protect yourself from Ransomware: Mitigation

Enterprise Defense

- Do not open suspicious or unexpected links or attachments in emails
- Hover over hyperlinks in emails to verify they are going to the anticipated site
- Alert your IT staff if you have any concerns about the legitimacy of any email, attachment, or link
- Be aware of malicious actors attempting to impersonate legitimate staff, and check the email sender name against the sender's email address
- Use unique strong passwords or pass-phrases for all accounts as well as multi-factor authentication
- Do not provide personal or organizational information unless you are certain of the requestor's identity
- Take advantage of available cybersecurity awareness training
- Ensure all data and systems critical to enterprise operations are regularly backed up at appropriate intervals
- Secure data back ups in accessible locations, and ensure the applicable restoration /operational status is conducive to a reasonable time frame to alleviate delayed network productivity.

- Only allow authentication to remote access software from inside the provider's network
- Continuous monitoring and logging should be used to monitor connections to MSP
- Maintain clear and updated picture of what is "normal" on your network
- Use two-factor authentication on remote administration tools and Virtual Private Network (VPN) tunnels rather than remote desktop protocols (RDPs)
- Block inbound network traffic from Tor exit nodes and outbound traffic to Pastebin
- Utilize Endpoint Detection and Response (EDR) to detect Powershell running unusual processes

Managed Service Providers (MSP's)





HHS 405(d)

Aligning Health Care
Industry Security Approaches



Healthcare & Public Health
Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

Resources

H-ISAC Industry Perspective

- ▶ Sharing best practices for ransomware prevention
 - Training & Awareness
 - Hardened defenses
- ▶ Health Industry Cybersecurity Practices (HICP)
- ▶ Sharing Indicators of Compromise
 - Provides early warning and protection for the HPH community
- ▶ Sharing Incident Information
 - Community awareness
 - Drives development of new strategies at the sector level



<https://h-isac.org/>



This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) task group member each iteration and do not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute this webinar series.

DHS Resources

- ▶ <https://www.cisa.gov>
- ▶ <https://www.us-cert.gov/Ransomware>
- ▶ https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf
- ▶ <https://www.cisa.gov/cyber-essentials>
- ▶ <https://www.us-cert.gov/report>
- ▶ <https://www.dhs.gov/be-cyber-smart>



DHS Resources



CYBER ESSENTIALS VOL. 1

Your success depends on *Cyber Readiness*. Both depend on **YOU**.

THE LEADER'S GUIDE

Reducing your organization's cyber risks requires a holistic approach - similar to the approach you would take to address other operational risks. As with other risks, cyber risks can threaten:



YOUR ABILITY TO OPERATE / ACCESS INFO



YOUR REPUTATION / CUSTOMER TRUST



YOUR BOTTOM LINE



YOUR ORGANIZATION'S SURVIVAL

Managing cyber risks requires building a culture of cyber readiness.

Essential Elements of a Culture of Cyber Readiness:

Yourself - The Leader

Drive cybersecurity strategy, investment and culture



Your awareness of the basics drives cybersecurity to be a major part of your operational resilience strategy, and that strategy requires an investment of time and money.
Your investment drives actions and activities that build and sustain a culture of cybersecurity.

Your Staff - The Users

Develop security awareness and vigilance



Your staff will often be your first line of defense, one that must have - and continuously grow - the skills to practice and maintain readiness against cybersecurity risks.

Your Systems - What Makes You Operational

Protect critical assets and applications



Information is the life-blood of any business; it is often the most valuable of a business' intangible assets.
Know where this information resides, know what applications and networks store and process that information, and build security into and around these.

Your Surroundings - The Digital Workplace

Ensure only those who belong on your digital workplace have access



The authority and access you grant employees, managers, and customers into your digital environment needs limits, just as those set in the physical work environment do.
Setting approved access privileges requires knowing who operates on your systems and with what level of authorization and accountability.

Your Data - What the Business is Built On

Make backups and avoid the loss of information critical to operations



Even the best security measures can be circumvented with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted.
Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.

Your Actions Under Stress

Limit damage and quicken restoration of normal operations



The strategy for responding to and recovering from compromise: plan, prepare for, and conduct drills for cyberattacks as you would a fire. Make your reaction to cyberattacks and system failures an extension of your other business contingency plans.
This requires having established procedures, trained staff, and knowing how - and to whom - to communicate during a crisis.

VOL.1 FALL 2019

[CISA.gov/Cyber-Essentials](https://www.cisa.gov/Cyber-Essentials)

For tech specs on building a Culture of Cyber Readiness, flip page ▶



DHS Resources



Backup Data
 Employ a backup solution that automatically and continuously backs up critical data and system configurations.

Multi-Factor Authentication
 Require multi-factor authentication (MFA) for accessing your systems whenever possible. MFA should be required of all users, but start with privileged, administrative and remote access users.

Patch & Update Management
 Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly.



THE IT PROFESSIONAL'S GUIDE

✓ *Actions for leaders.*
 ✓ *Discuss with IT staff or service providers.*

Essential Actions for Building a *Culture of Cyber Readiness*:

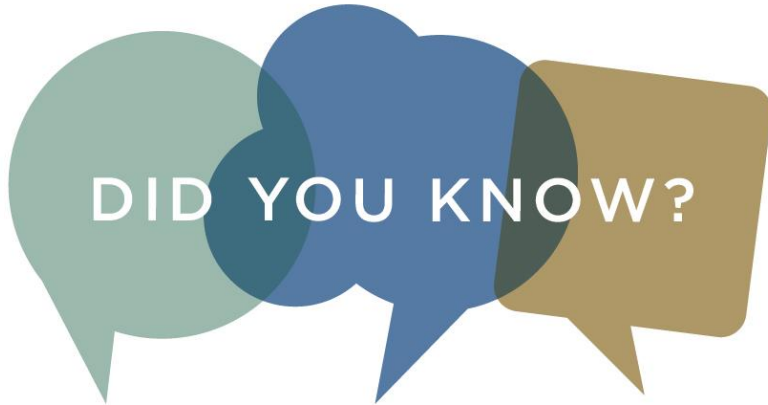
Youself Drive cybersecurity strategy, investment and culture	Your Staff Develop security awareness and vigilance	Your Systems Protect critical assets and applications	Your Surroundings Ensure only those who belong on your digital workplace have access	Your Data Make backups and avoid loss of info critical to operations	Your Actions Under Stress Limit damage and quicken restoration of normal operations
<p><i>Organizations living the culture have:</i></p> <ul style="list-style-type: none"> ✓ Lead investment in basic cybersecurity. ✓ Determined how much of their operations are dependent on IT. ✓ Built a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information. ✓ Approached cyber as a business risk. ✓ Lead development of cybersecurity policies. 	<p><i>Organizations living the culture have:</i></p> <ul style="list-style-type: none"> ✓ Leveraged basic cybersecurity training to improve exposure to cybersecurity concepts, terminology and activities associated with implementing cybersecurity best practices. ✓ Developed a culture of awareness to encourage employees to make good choices online. ✓ Learned about risks like phishing and business email compromise. ✓ Identified available training resources through professional associations, academic institutions, private sector and government sources. ✓ Maintained awareness of current events related to cybersecurity, using lessons-learned and reported events to remain vigilant against the current threat environment and agile to cybersecurity trends. 	<p><i>Organizations living the culture have:</i></p> <ul style="list-style-type: none"> ✓ Learned what is on their network. Maintained inventories of hardware and software assets to know what is in-play and at-risk from attack. ✓ Leveraged automatic updates for all operating systems and third-party software. ✓ Implemented secure configurations for all hardware and software assets. ✓ Removed unsupported or unauthorized hardware and software from systems. ✓ Leveraged email and web browser security settings to protect against spoofed or modified emails and unsecured webpages. ✓ Created application integrity and whitelisting policies so that only approved software is allowed to load and operate on their systems. 	<p><i>Organizations living the culture have:</i></p> <ul style="list-style-type: none"> ✓ Learned who is on their network. Maintained inventories of network connections (user accounts, vendors, business partners, etc.). ✓ Leveraged multi-factor authentication for all users, starting with privileged, administrative and remote access users. ✓ Granted access and admin permissions based on need-to-know and least privilege. ✓ Leveraged unique passwords for all user accounts. ✓ Developed IT policies and procedures addressing changes in user status (transfers, termination, etc.). 	<p><i>Organizations living the culture have:</i></p> <ul style="list-style-type: none"> ✓ Learned what information resides on their network. Maintained inventories of critical or sensitive information. ✓ Established regular automated backups and redundancies of key systems. ✓ Learned how their data is protected. ✓ Leveraged malware protection capabilities. ✓ Leveraged protections for backups, including physical security, encryption and offline copies. ✓ Learned what is happening on their network. Managed network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities. 	<p><i>Organizations living the culture have:</i></p> <ul style="list-style-type: none"> ✓ Lead development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often. ✓ Leveraged business impact assessments to prioritize resources and identify which systems must be recovered first. ✓ Learned who to call for help (outside partners, vendors, government / industry responders, technical advisors and law enforcement). ✓ Lead development of an internal reporting structure to detect, communicate and contain attacks. ✓ Leveraged in-house containment measures to limit the impact of cyber incidents when they occur.

VOL. 1 FALL 2019

Consistent with the NIST Cybersecurity Framework and other standards, these actions are the starting point to Cyber Readiness. To learn more, visit [CISA.gov/Cyber-Essentials](https://www.cisa.gov/Cyber-Essentials).

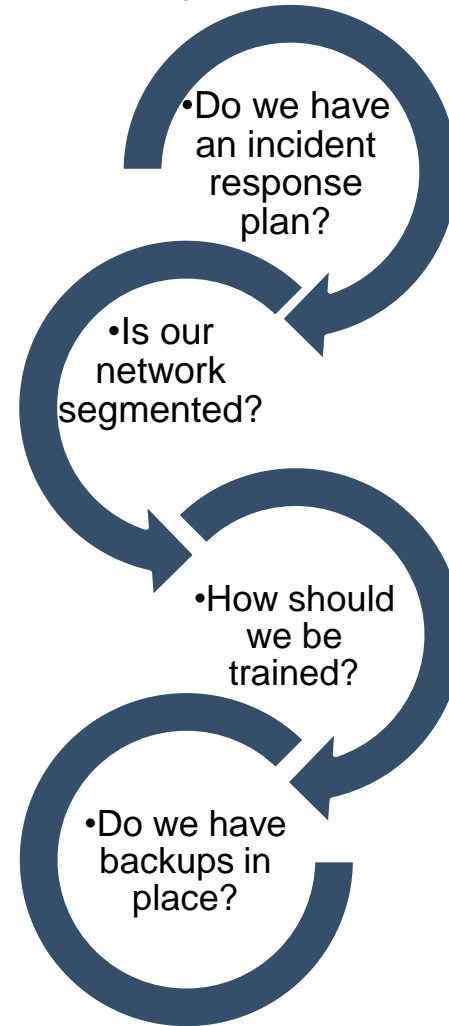


Ransomware - What You Can Do



- Most Ransomware attacks begin in email phishing attacks asking you to click or open an attachment
- Always follow the correct Email Phishing tips and double check the email sender's credentials prior to opening attachments

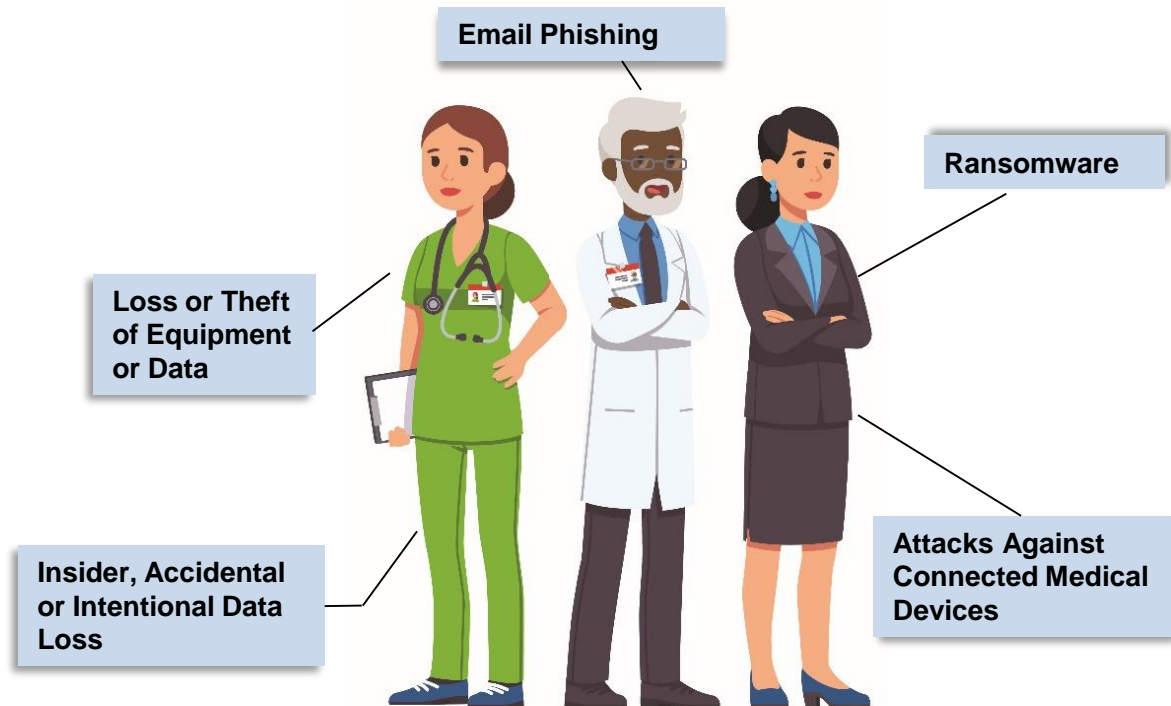
What to ask your IT Professionals:



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

After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a **main document** and **two technical volumes**, and a robust appendix of **resources and templates**

The Five Main Threats in Cybersecurity





HHS 405(d)

Aligning Health Care
Industry Security Approaches



Healthcare & Public Health
Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

Questions

Closing

For more cybersecurity information and best practices, be sure to check out the 405(d) publication titled:

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

The publication details the top five threats facing the healthcare industry and the top 10 practices to mitigate. Read the entire publication on our website: www.phe.gov/405d.

Next 405(d) Spotlight Webinar:

February 2020; Date and time to be released later this month

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) task group member each iteration and do not reflect the views of HHS as a whole. All task group members have been invited to contribute this webinar series.



Thank you for joining us!

Visit us at: www.phe.gov/405d

Contact us at: CISA405d@hhs.gov



Helpful Links

HHS 405(d)

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

HHS HC3

HC3 Sodinokibi Ransomware Whitepaper

HC3 Briefing: Ransomware Threat to State and Local Governments

DHS

<https://www.cisa.gov>

<https://www.us-cert.gov/Ransomware>

<https://www.us->

[cert.gov/sites/default/files/2019-](https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-)

[08/CISA_Insights-](https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-)

[Ransomware_Outbreak_S508C.pdf](https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf)

<https://www.cisa.gov/cyber-essentials>

<https://www.us-cert.gov/report>

<https://www.dhs.gov/be-cyber-smart>

