LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

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

April 2019

Jigar Kadakia
Chief Information Security and Privacy Officer
jkadakia@partners.org

PARTNERS HEALTHCARE | FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL AND MASSACHUSETTS GENERAL HOSPITAL

- 20-years plus in health information management
- Health ISAC-Board Member
- Certified Information Systems Security Professional (CISSP) ISC^2
- Certified Privacy Professional (CIPP)
- National Medical Device Taskforce
- JAMA Network Paper-Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions

Karen Greenhalgh
karen@cybertygr.com

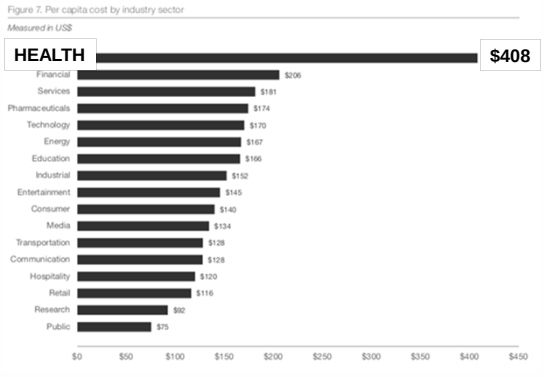
- Certified in Healthcare Privacy Compliance (CHPC)
- Certified in Healthcare Compliance (CHC)
- Healthcare Information Systems & Privacy Practitioner (HCISPP) ISC^2
- Founder Cyber Tygr
- HHS led CISA 405(d) task group member
- Healthcare and Public Health Sector Coordinating Counsel Joint Cybersecurity
- NCHICA Privacy and Security Taskforce

HEALTHCARE – HACKERS #1 TARGET

"Bummer of a birthmark, Hal."

- ❑ Most valuable record - $500/record
- ❑ Least investment in cybersecurity
- ❑ Lack of qualified personnel
- ❑ Medical Devices & IoT (Internet of Things)
- ❑ Patient Safety Issues

Cost of a Data Breach – per record

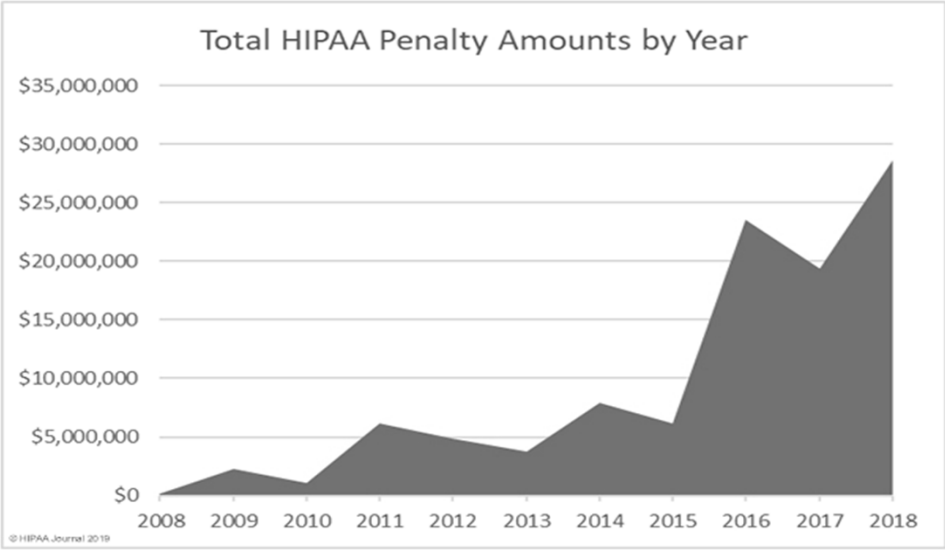


- Civil Money Penalties
- Interrupt critical business operations
- Reduction in credit worthiness
- Reputation
- Loss of future business
- Patient Safety

2018 Cost of a Data Breach: Ponemon Institute

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

Healthcare Breach and Incident Volumes



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

Typical HIPAA Violations

1. Risk Analysis was not thorough
2. Lack of safeguards
3. Failure to report breach
4. Use and disclosure issues
5. Missing or deficient policies and procedures
6. Outdated or insufficient training
7. Inconsistent access monitoring
8. 3rd party disclosure
9. Lost or stolen device – laptop, USB, smart phone
10. Lack of encryption

2019 Forecasts & Statistics

- Robert Herjavek – large infosec company
  - **300% increase in attacks** on healthcare
- ECRI – scientific analysis
  - **25% of healthcare attacks** from RDP
  - **Connected Medical Device** #1 Hazard 2019
- Regulations and Oversight will increase – FTC Civil Fines, US GDPR, HIPAA Revisions
- OCR considering increasing investigations – 3rd Party and Spot Audits
- One in three hospitals will experience a cybersecurity incident w/in 2 years
- OCR – **89%** of ePHI enforcement actions cited **Risk Analysis Failure**
- HIMSS – **80% experienced significant cybersecurity** issue in the last 12 months
- Supply Chain or **3rd Party Vendor attacks up 78%** in 2018 - Covered Entity exposure

Christopher Wray – Director FBI

March 5th, 2019

"Today's cyberthreat is bigger than any one government agency — in fact it's bigger than the government itself," Wray said. "The scope, breadth, depth, sophistication and diversity of the threat we face now is unlike anything we've had in our lifetimes."

MeriTalk
Improving the Outcomes of Government IT

Neilson Calls for "Whole of Society" Effort on Cyber

March 18th, 2019

"What worries me is not what these threat actors have done, but what they have the capability to do," she noted. "The possibilities are limitless, but the time we have to prepare is not."

Mal-ware

MALICIOUS SOFTWARE

[redacted]

[redacted]

NIST USE

OUI TAM

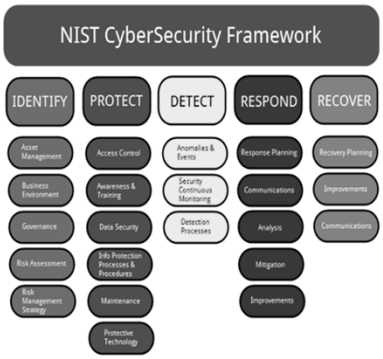
BUSINESS ASSOCIATE

INSIDE CYBERSECURITY

DAILY NEWS

Senate panel eyes mandating use of NIST cyber framework following Equifax investigation

March 06, 2019 | **Rick Weber**



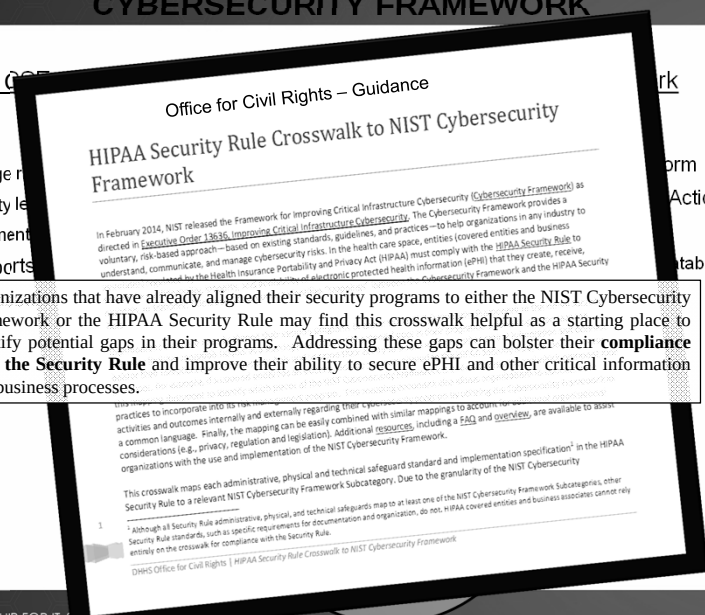
LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

18

NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY CYBERSECURITY FRAMEWORK

NIST C… …rk

- Goal
  - Manage r… …orm
  - Maturity le… …Action, Impact
  - Implement…
- HHS supports… …table, Adaptive
- HIPA…



Office for Civil Rights – Guidance

HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as directed in Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The Cybersecurity Framework provides a voluntary, risk-based approach—based on existing standards, guidelines, and practices—to help organizations in any industry to understand, communicate, and manage cybersecurity risks. In the health care space, entities (covered entities and business …

practices to incorporate into its risk … activities and outcomes internally and externally regarding their cybersecurity … a common language. Finally, the mapping can be easily combined with similar mappings to account for … considerations (e.g., privacy, regulation and legislation). Additional resources, including a FAQ and overview, are available to assist organizations with the use and implementation of the NIST Cybersecurity Framework.

This crosswalk maps each administrative, physical and technical safeguard standard and implementation specification[1] in the HIPAA Security Rule to a relevant NIST Cybersecurity Framework Subcategory. Due to the granularity of the NIST Cybersecurity

[1] Although all Security Rule administrative, physical, and technical safeguards map to at least one of the NIST Cybersecurity Framework Subcategories, other Security Rule standards, such as specific requirements for documentation and organization, do not. HIPAA covered entities and business associates cannot rely entirely on the crosswalk for compliance with the Security Rule.

DHHS Office for Civil Rights | HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

Organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule may find this crosswalk helpful as a starting place to identify potential gaps in their programs. Addressing these gaps can bolster their **compliance with the Security Rule** and improve their ability to secure ePHI and other critical information and business processes.

LEADERSHIP FOR IT S… …ROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

19

Cybersecurity Act of 2015 (CSA)

CSA Section 405

Improving Cybersecurity in the Health Care Industry

- Section 405(b): Health care industry preparedness report
- Section 405(c): Health Care Industry Cybersecurity Task Force
- **Section 405(d): Aligning Health Care Industry Security Approaches**

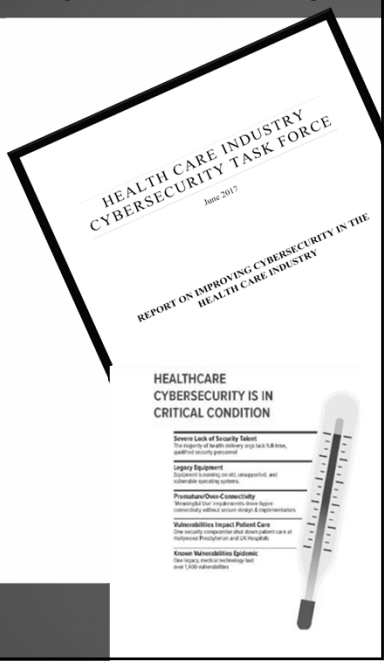
LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

20

405(c) Health Care Industry Cybersecurity Task Force Report

6 IMPERATIVES

1. **NIST CSF for leadership and governance**
2. **Security and resilience increased**
   - ❖ medical devices & Health IT
3. **Improve information sharing**
   - ❖ threats, weaknesses, and mitigations
4. **Cybersecurity training & awareness**
5. **Develop workforce**
6. **Protect R&D and Intellectual Property**

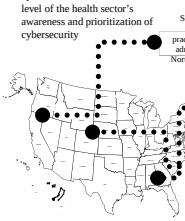


405(d) - Aligning Health Care Industry Security Approaches

Medical Community Baseline

Qualitative research to establish the level of the health sector's awareness and prioritization of cybersecurity

Series of one-on-one interviews with practitioners and practice administrators from the Northwest, Northeast, and Southeast



7 Focus Group
4 in-person
3 virtual

Qualitative Research with medical professionals, HPH, CIOs/CISOs etc.

2017 HHS convened the 405(d) Task Group leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership.

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Who is Participating

The 405(d) Task Group is convened by HHS and comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders.

What is the 405(d) Initiative?

An industry-led process to develop consensus-based guidelines, practices, and methodologies to strengthen the HPH-sector's cybersecurity posture against cyber threats.

Our Mandate

To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d).

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

- ✓ The four-volume publication includes a main document, two technical volumes, and resources and templates aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector.

405(d) Start

Pretest

National Pretesting sessions were both in-person and virtual, and feedback was gathered with focus groups of 9-15 participants via roundtable discussion. A total of 123 took part in the pretesting efforts

Release

Future

- ✓ Become the leading collaboration center for developing healthcare cybersecurity focused resourced
- ✓ Continue to build upon the HICP publication
- ✓ Develop new cybersecurity resources

Healthcare Industry Cybersecurity Practices (HICP)

HICP is…

- A call to action to manage real cyber threats
- Written for multiple audiences (clinicians, executives, and technical)
- Designed to account for organizational size and complexity (small, medium and large)
- A reference to "get you started" while linking to other existing knowledge
- Aligned to the NIST Cybersecurity Framework
- Voluntary

HICP is **not**…

- A new regulation
- An expectation of minimum baseline practices to be implemented in all organizations
- The definition of "reasonable security measures" in the legal system
- An exhaustive evaluation of all methods and manners to manage the threats identified
  - You might have other practices in place that are more effective than what was outlined!
- Your guide to HIPAA, GDPR, State Law, PCI, or any other compliance framework

Documentation Overview

- **Main Document**
  - Industry cybersecurity threats and vulnerabilities
  - Explores five (5) current threats
  - Presents ten (10) practices to mitigate those threats
- **Technical Volume 1**
  - Small healthcare organization
  - Ten (10) detailed cybersecurity mitigation practices
  - Nineteen (19) detailed sub-practices
- **Technical Volume 2**
  - Medium and Large healthcare organizations
  - Ten (10) detailed cybersecurity mitigation practices
  - Seventy (70) detailed sub-practices
- ***Resources and Templates***
  - Mappings to the NIST Cybersecurity Framework
  - An HICP assessment process
  - Sample Templates
  - Acknowledgements for its development.

5 Current Threats

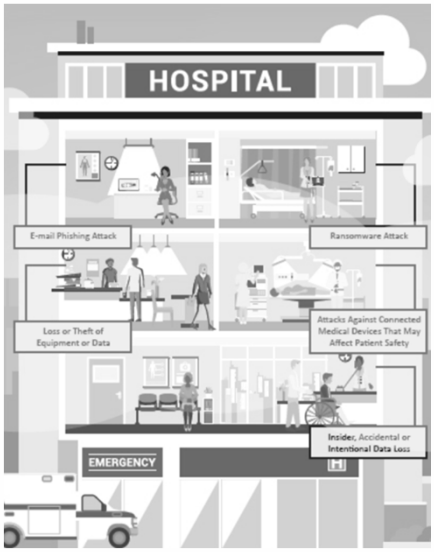
1. **Email Phishing Attacks**
2. **Ransomware Attacks**
3. **Loss or Theft of Equipment or Data**
4. **Internal, Accidental, or Intentional Data Loss**
5. **Attacks Against Connected Medical Devices that May Affect Patient Safety**

https://www.cybertygr.com/resource

https://www.phe.gov/405d

Ten (10) Cybersecurity Mitigation 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 & SOC
9. Medical Device Security
10. Cybersecurity Policies



Email Phishing – Small Organization

Practice	Sub-Practice	To Consider	NIST Reference
E-mail Protection Systems	(1.S.A): E-mail System Configuration	• Tag external e-mails to make them recognizable to staff • Implement multifactor authentication (MFA)	NIST FRAMEWORK REF: PR.DS-2, PR.IP-1, PR.AC-7
Email Protection Systems	(1.S.B): Education	• Be suspicious of e-mails from unknown senders, e-mails that request sensitive information such as PHI or personal information, or e-mails that include a call to action that stresses urgency or Importance • Train staff to recognize suspicious e-mails and to know where to forward them • Never open e-mail attachments from unknown enders	NIST FRAMEWORK REF: PR.AT-1
Email Protection Systems	(1.S.C): Phishing Simulations	• Implement proven and tested response procedures when employees click on phishing e-mails	NIST FRAMEWKORK REF: PR.AT
Incident Response	(8.S.B): ISAC/ISAO Participation	• Establish cyber threat information sharing with other health care organizations	NIST: DETECT - ID.RA-2

Email Phishing
Medium/Large Organization

Cybersecurity Practice 1: E-mail Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	1.M.A 1.M.B 1.M.C 1.M.D	Basic E-mail Protection Controls Multifactor Authentication for Remote Access E-mail Encryption Workforce Education
Large Sub-Practices	1.L.A 1.L.B 1.L.C	Advanced and Next-Generation Tooling Digital Signatures Analytics Driven Education
Key Mitigated Risks	• E-mail Phishing Attacks • Ransomware Attacks • Insider, Accidental or Intentional Data Loss	

What Size is My Organization?

Implement resources and practices tailored and cost effective

Factors Determining Size:

- Health Information Exchanges
- IT Capability
- Cybersecurity Investment
- Size (provider)
- Size (acute/post-acute)
- Size (hospital)
- Complexity

Main Document – page 11

Best Fit		Small	Medium	Large
Common Attributes	Health information exchange partners	One or two partners	Several exchange partners	Significant number of partners or partners with less rigorous standards or requirements Global data exchange
	IT capability	No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by project-basis	Dedicated IT resources on staff No or limited dedicated security resources on staff	Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Nonexistent or limited funding	Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity and IT budgets are blended	Dedicated budget with strategic roadmap specific to cybersecurity
Provider Attributes	Size (provider)	1–10 physicians	11–50 physicians	Over 50 physicians
	Size (acute / post-acute)	1–25 providers	26–500 providers	Over 500 providers
	Size (hospital)[15]	1–50 beds	51–299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated delivery networks Participate in accountable care organization or clinically integrated network
Other Org Types			Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations	Health Plan Large Device Manufacturer Large pharmaceutical organization

Table 1. Selecting the "Best Fit" For Your Organization

Self Assessment - Practices & Sub Practices

FULL LISTING OF CYBERSECURITY SUB-PRACTICES BASED ON ORGANIZATION SIZE SELECTED			Self Assessment			
SP#	Cybersecurity Sub-Practice Title	Short Description	Current State	Gaps	Action Plan	Priority
2.M.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	*Encryption at 80%, AV in place, baseline image, all users with admin rights*	*Encryption gaps and admin rights*	*Finish encryption, remove admin rights*	*High*
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record	*All users provided accounts, not tied to ERP*	*No identity, can allow for orphaned accounts and failure to term*	*Establish identity program*	*Me*
3.M.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination	*User accounts created directly into Active Directory manually, when requested*	*Access rights might cumulate and administrators might fail to terminate access*	*Establish accounts based upon identity, automate provisioning and de-provisioning*	*Med*
3.M.C	Authentication	Implement and monitor secure authentication for users and privileged accounts	*Authentication bound to central authentication source*	*No gaps*	*No gaps*	*N/A*
3.M.D	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources	*VPN access available, no MFA*	*No MFA enabled, which can allow for a theft of credentials to access sensitive data*	*Implement MFA*	*Med*
8.M.A	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks	*Dedicated team to manage and respond to cyber incidents*	*No gaps*	*No Gaps*	*N/A*
8.M.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks	*Playbooks exist, but no playbook for lost/stolen device*	*In the case of a stolen device teams might not execute investigation properly*	*Establish playbook for stolen devices, get approval from leadership*	*High*
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information	*Not a current member of an ISAC/ISAO*	*By not participating in ISAC/ISAOs cyber teams might be missing out on leading practices*	*Join ISAC/ISAO*	*High*

Cybersecurity Practices Assessment Toolkit

Prioritization Tool

- Approach
  - Threat - apply combination of Practices and Sub-Practices
  - Practice - applicable to multiple Threats

Factor		
Select your organizations size		Medium
Prioritize the threats (5 being highest priority, 1 being lowest priority)		
A	Email Phishing Attack	1
B	Ransomware Attack	4
C	Loss or Theft of Equipment or Data	5
D	Insider, Accidental or Intentional Data Loss	3
E	Attacks Against Connected Medical Devices that may affect Patient Safety	2

CP #	Cybersecurity Practices	Priority Rank Based on Threat Model Inputs
8	Incident Response	28
3	Access Management	23
2	Endpoint Protection Systems	23
5	Asset Management	20
6	Network Management	16
7	Vulnerability Management	16
10	Cybersecurity Policies	15
1	Email Protection Systems	13
9	Medical Device Security	11
4	Data Protection and Loss Prevention	11

HICP is a Cookbook!

So you want a recipe for Medium to Large Phish?

1. 5 oz of Basic E-Mail Protection Controls (1.M.A)
2. A dash of Multi-Factor Authentication (1.M.B)
3. 2 cups of Workforce Education (1.M.D)
4. 1 cup of Incident Response plays (8.M.B)
5. 1 tsp of Digital Signatures for authenticity (1.L.B)
6. Advanced and Next General Tooling to taste (1.L.A)

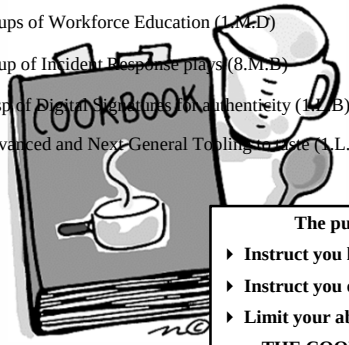
Preheat your email system with some basic email protection controls necessary to build the foundation of your dish

Mix in MFA for remote access, in order to protect against potential credential theft

Let sit for several hours, while providing education to your workforce on the new system, and how to report phishing attacks

While doing so, ensure to provide education on how digital signatures demonstrating authenticity of the sender

When finished baking, sprinkle with additional tooling to provide next level protection



The publication does not:

- **Instruct you how to cook**
- **Instruct you on what recipes to use**
- **Limit your ability for substitutions**

THE COOK MAKES THE DISH

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

31

CSA 405(d) - Looking Forward

- **Leading collaboration center of HHS Office of the CIO**
- **Partnership with HHS Divisions and the healthcare industry**
- **Develop resources to align health care cybersecurity practices**
- **Educate Industry**
- **HICP 2.0 – in development**

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

Thank you for joining us

Contact 405(d):
CISA405d@hhs.gov

Contact Cyber Tygr:
ty@cybertygr.com
www.cybertygr.com

33

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

Questions