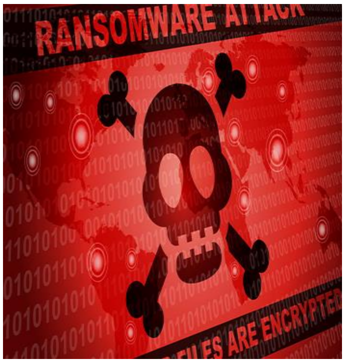


Health Industry Cybersecurity Practices

Managing Threats and Protecting Patients

HCCA Virtual Philadelphia Region

HACKERS CONVENTION

black hat®

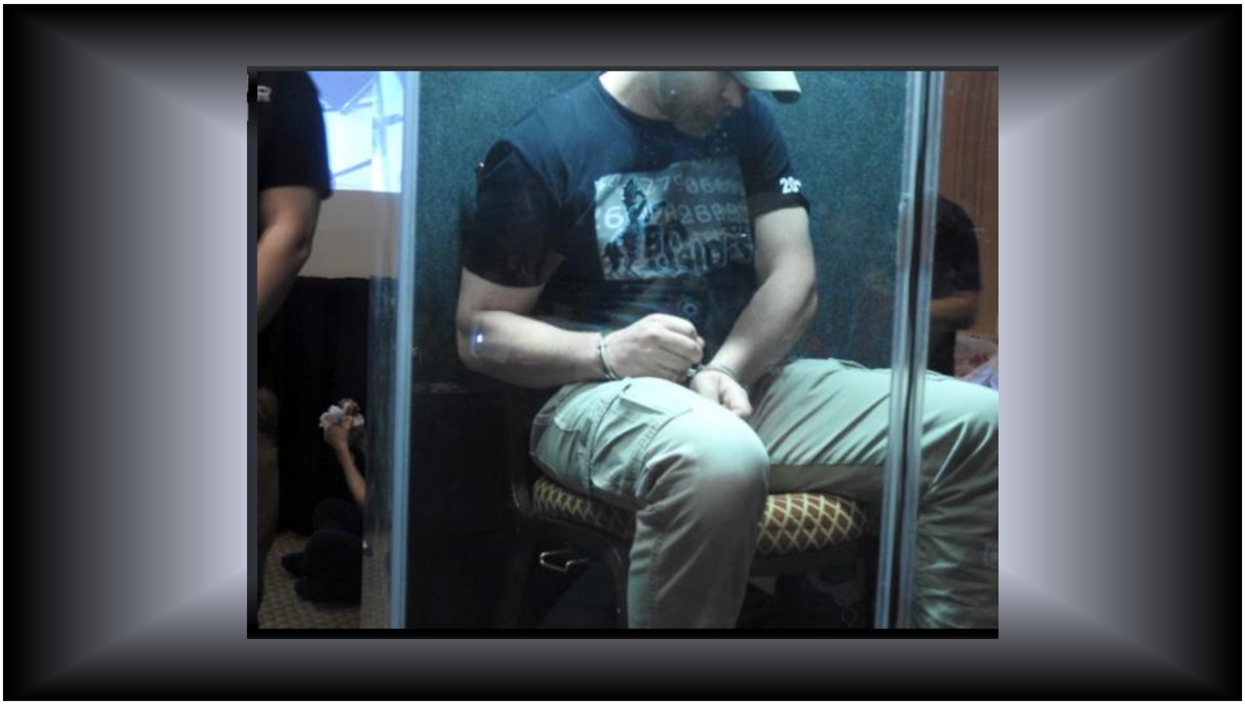
DEFCON®

50,000 Hackers in Attendance

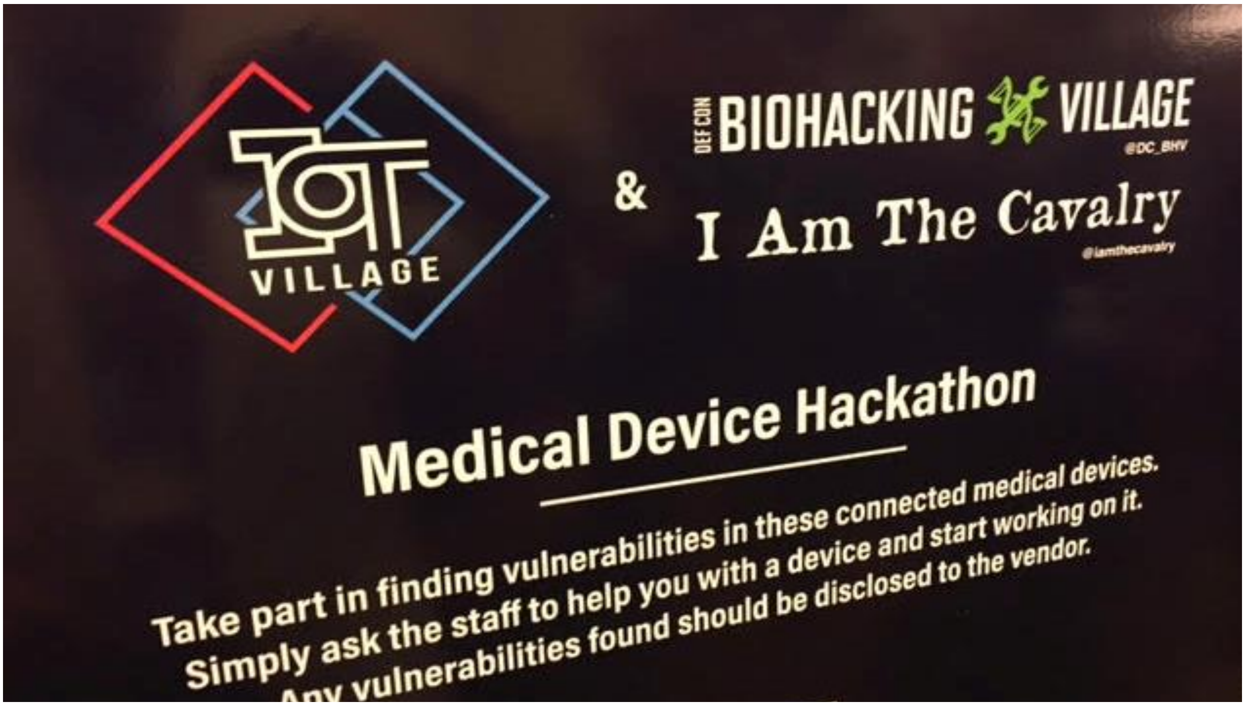
3

4

5



6



IoT VILLAGE

&

DEF CON BIOHACKING VILLAGE @DC_BHV

I Am The Cavalry @iamthecavalry

Medical Device Hackathon

Take part in finding vulnerabilities in these connected medical devices.
Simply ask the staff to help you with a device and start working on it.
Any vulnerabilities found should be disclosed to the vendor.

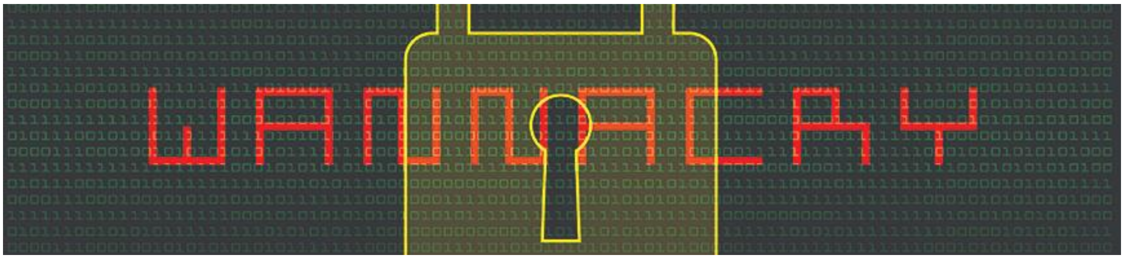
7

HACKING

KITS.
DEVICES.
LABS. TOOLS.
VIDEOS.
AND MORE.

ATTIFY

8

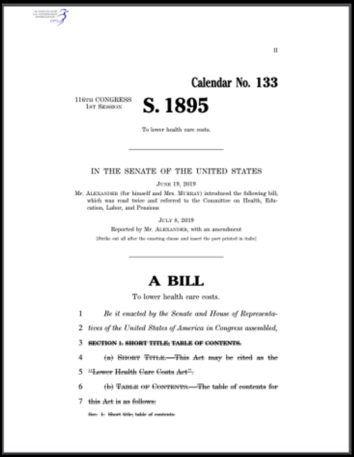


2017

- Windows Vulnerability
- 300,000 computers shut down
- One fifth of the UK Health System Shut Down

2020

- Urgent 11 – Sept 2019 (CVSS 9.8)
- BlueKeep – Wormable like Wannacry
- 49 Windows Vulnerabilities – Jan 2020
- Many more…….
- COVID 19 – Healthcare Industry (Critical)



II

Calendar No. 133

116th CONGRESS
1st Session

S. 1895

To lower health care costs.

IN THE SENATE OF THE UNITED STATES

June 19, 2019

Mr. Alexander (for himself and Mrs. Murray) introduced the following bill; which was read twice and referred to the Committee on Health, Education, Labor, and Pensions

July 8, 2019

Reported by Mr. Alexander, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To lower health care costs.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

~~**SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**~~

~~(a) Short Title.—This Act may be cited as the "Lower Health Care Costs Act".~~

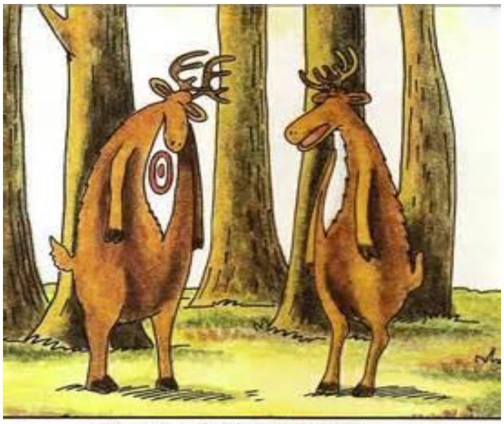
~~(b) Table of Contents.—The table of contents for this Act is as follows:~~

~~Sec. 1. Short title; table of contents.~~

Lower Health Care Costs Act – Section 502

- Senate Bill 1895
- Recognition of Security Practices
  - ***Approaches promulgated under section 405(d) of the Cybersecurity Act 2015***
- Reduce Breach Exposure
  - Mitigate fines
  - Early favorable termination of an audit
  - Limit remedies from HHS
- Documentation for 12 months

Healthcare – #1 Target

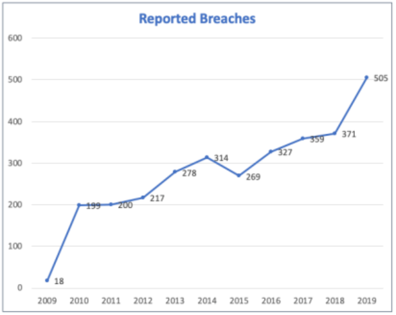


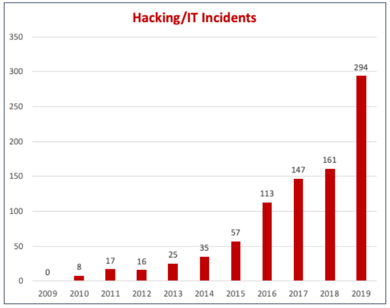
"Bummer of a birthmark, Hal."

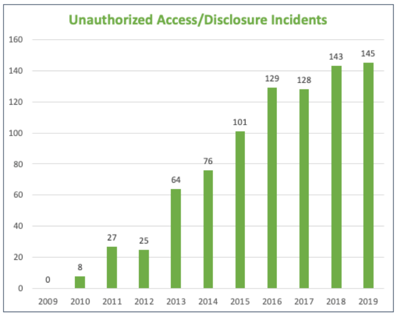
"FULLZ"

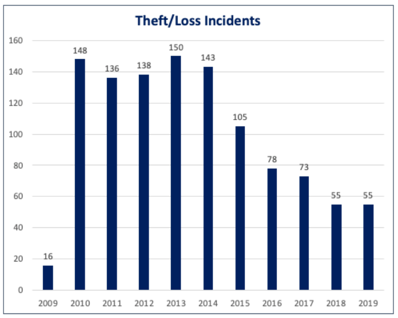
A compilation or package of information
on a prospective fraud or identity
theft victim.

- Most costly across industry - $408
- Most valuable record for hackers - $500
- Highest "Churn Rate" due to breach
- Longest "Identify and Contain" times – 358 days
- Records breached in 2019 increased 300% - 41 million
- Fines and Fees hit $28m in 2019
- Least investment in cybersecurity
- Medical Devices Security = Patient Safety









Everyone who works here
Everyone who doesn't work here
klossner
" WE'VE NARROWED OUR SECURITY RISKS DOWN to THESE TWO GROUPS."

13

13

14

14

HHS 405(d)
Aligning Health Care Industry Security Approaches

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Health Industry Cybersecurity Practices:

Managing Threats and Protecting Patients

"HICP"

2019 Winner FedHealthIT Innovation Awards

15

Ty Greenhalgh
ty@cybertygr.com

CYBER TYGR

- Co-founder Cyber Tygr
- 30 years experience in HIM
- Henry Ford Health System – Most Innovative Technology of the Year
- Healthcare Information Systems & Privacy Practitioner (HCISPP) ISC^2
- HHS Joint Cybersecurity Workgroup
- NCHICA Biomedical Security Taskforce
- HHS led CISA 405(d) task group member

PROUD MEMBER

16

16

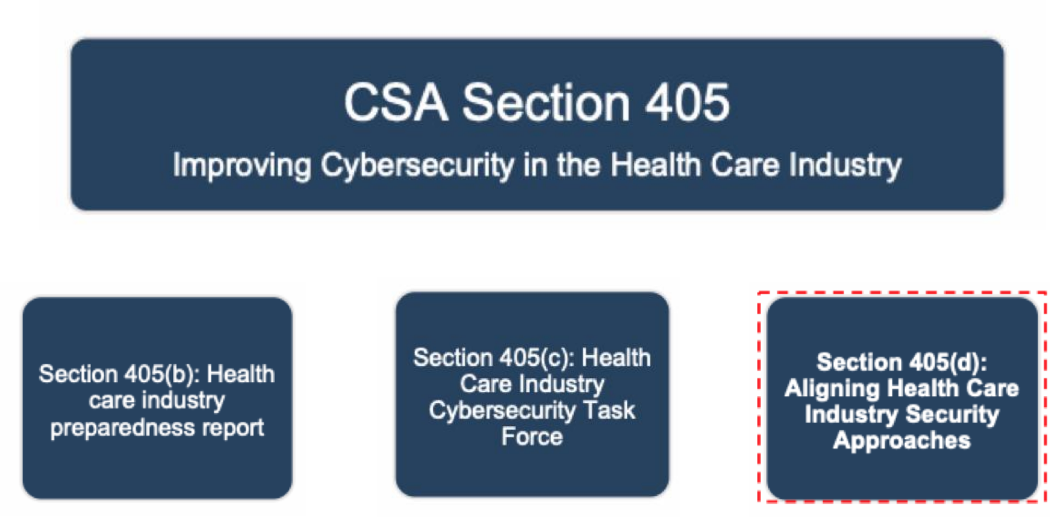
- Top 5 Current Threats
- 10 Mitigation Practices
- Traveling the 405
- Resources and Templates
- Where is the 405 going
- Questions

Agenda

17

17

Cybersecurity Act (CSA) 2015



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

18

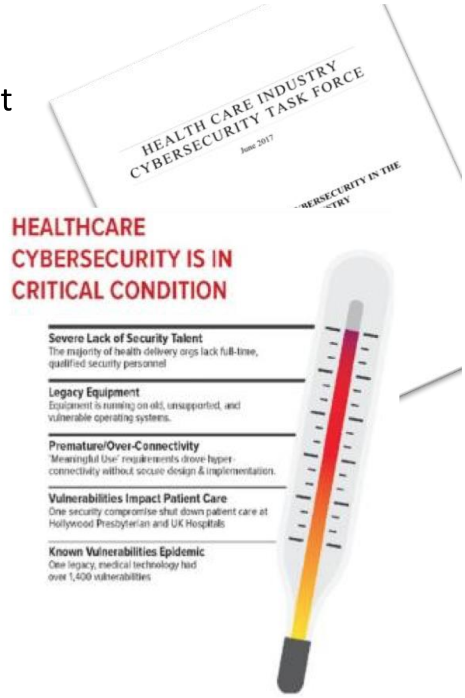
18

CSA 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
4. Cybersecurity training & awareness
5. Develop workforce
6. Protect R&D and Intellectual Property



HEALTH CARE INDUSTRY
CYBERSECURITY TASK FORCE

June 2017

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

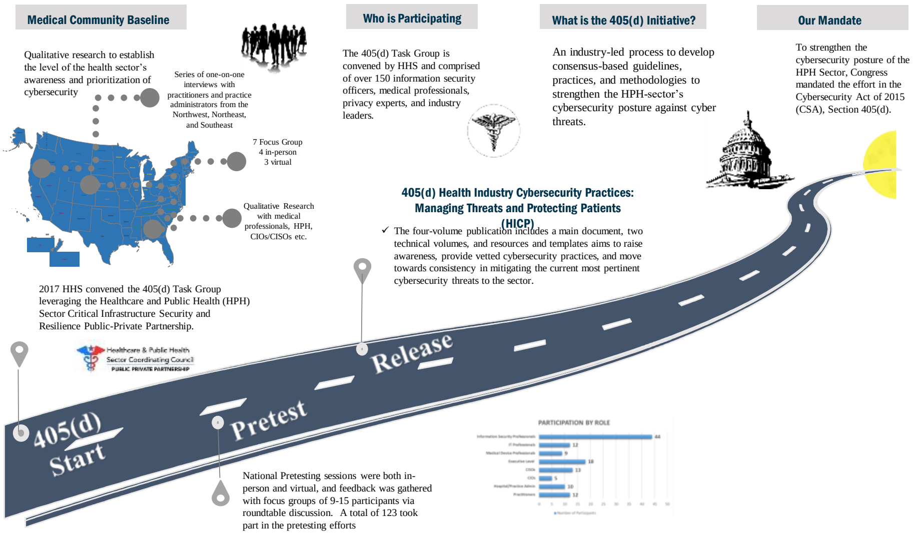
Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

CSA 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.

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

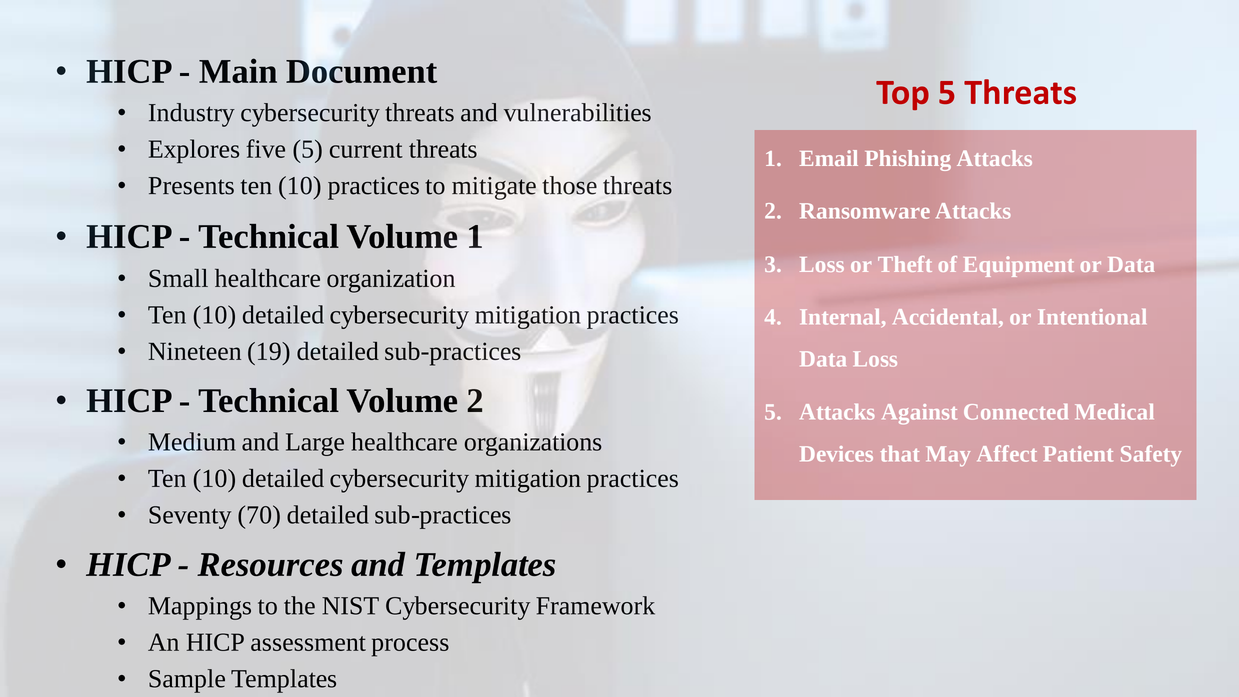
To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d).

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.

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

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP
405(d) Start
Pretest
Release
PARTICIPATION BY ROLE
Information Security Professionals 44
IT Professionals 12
Medical Device Professionals 9
Executive Level 18
CISOs 13
CIOs 5
Hospital/Practice Admin 10
Practitioners 12
0 5 10 15 20 25 30 35 40 45 50
Number of Participants



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

Top 5 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**

21

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

22

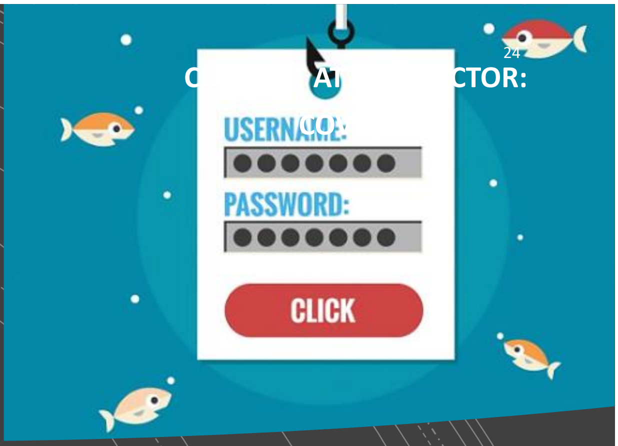
22

Top 5 Threats

23

#1 Threat

RomoloTavani / Getty Images / Thinkstock



Email Phishing Attack

- Spear Phishing
- Executive Whaling
- Social Engineering
- Malvertising

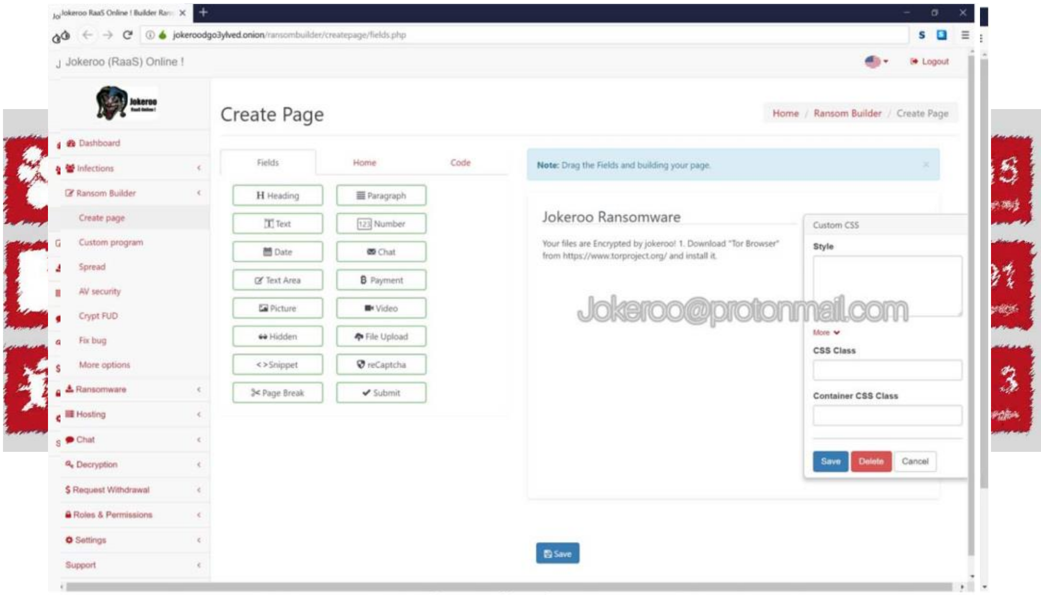
24

#2 Threat

Ransomware

- Email
- Drive by Download
- Free Software
- Remote Desktop Protocol (RDP)
- Ransom - Bitcoin
- Held Hostage

Ransomware-As-A-Service



jokeroodgo3ylved.onion/ransombuilder/createpage/fields.php

Create Page

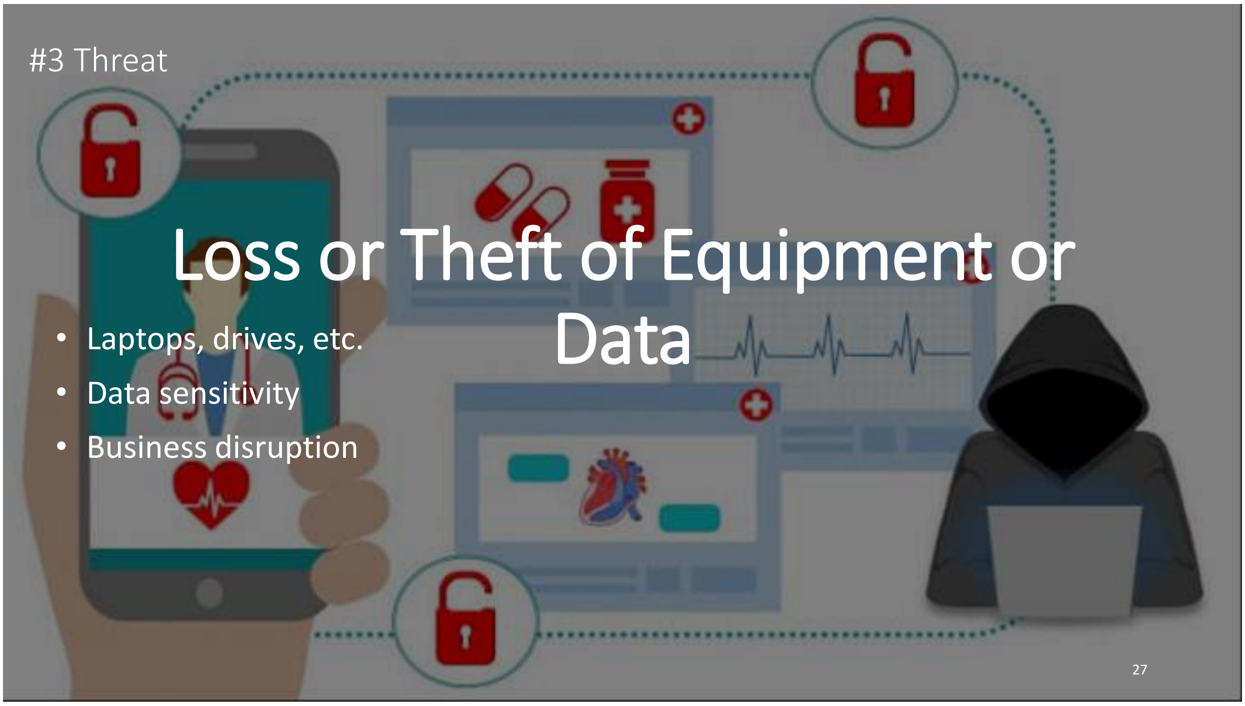
Note: Drag the Fields and building your page.

Jokeroo Ransomware

Your files are Encrypted by jokeroo! 1. Download "Tor Browser" from https://www.torproject.org/ and install it.

Jokeroo@protonmail.com

Ransom Note Creator



#3 Threat

Loss or Theft of Equipment or Data

- Laptops, drives, etc.
- Data sensitivity
- Business disruption

27

27

#4 Threat

Insider – Accidental or Intentional Data Loss

- Accidental Insider
  - Honest mistakes
  - Procedural errors
  - Emailing sensitive data
- Intentional Insider
  - Personal gain
  - Inflict harm
  - Impersonating staff
  - Disgruntled employee

28

#5 Threat

Medical Device Security: Patient Safety

- Inventory control
- Software patches
- Device monitoring
- Remote access
- Anti-malware
- Urgent 11 – VxWorks OS

Top 10 Cybersecurity Practices

Top 10 Cybersecurity Practices

Doctors and nurses know that hand sanitizing is critical to prevent the spread of germs. That does not mean healthcare workers wash up as often as they should.

Similarly, cybersecurity practices reduce the risk of cyber-attacks and data breaches. Just as we are able to protect our patients from infection, we should all work towards protecting patient data to allow physicians and caregivers to trust the data and systems that enable delivery of quality health care.

Cyber Hygiene

Patient Safety

Email Protection Systems

- Education
- Phishing Simulation
- E-mail Protection Controls
- Domain Key Identified Mail (DKIM)
- E-mail Encryption

Endpoint Protection Systems

- Micro-segmentation
- Mobile Device Management
- Host Based Intrusion Detection/Prevention Systems
- Endpoint Detection and Response
- Application Whitelisting

#2 Practice

33

Access Management

- Identity
- Automate Provisioning
- Authentication
- Multifactor Authentication for Remote Access
- Single-Sign On

34

Data Protection and Loss Prevention

- Policies & Procedures
- Classification of Data
- Data Use Procedures
- Data Security
- Backup Strategies
- Data Loss Prevention
- Mapping of Data Flows

#4 Practice

35

Asset Management

- Inventory Details
- Decommissioning
- Automated Discovery and Maintenance
- Procurement – HIC-SCRiM

https://healthsectorcouncil.org/hic-scrim/

#5 Practice

36

Network Management

#6 Practice

- Network Segmentation
- Physical Security
- Intrusion Prevention
- Network Profiles and Firewalls
- Network Access Control

37

Vulnerability Management

- Scanning
- Data Classification
- Patch Management
- Configuration Management
- Penetration Testing

#6 Practice

38

Incident Response

- Incident Response
- ISAC/ISAO Participation
- Security Operations Center (SOC)
- Baseline Network Traffic
- User Behavior Analytics
- Deception Technologies

#8 Practice

Medical Device Security

- Procurement and Security Evaluations
- Practice #2
- Practice #3
- Practice #5
- Practice #6
- Practice #7
- Practice #8
- Practice #10
- Contacting the FDA

#9 Practice

Cybersecurity Policies

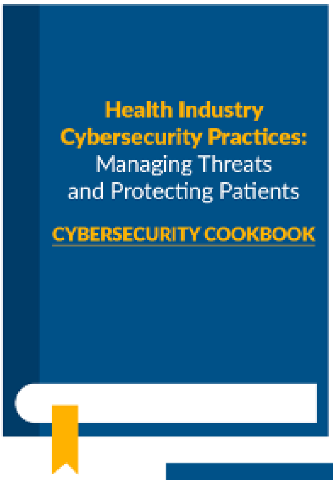
- Policies

#10 Practice

41

41

So You Want A Recipe For Cybersecurity?


Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

CYBERSECURITY COOKBOOK

Mitigating Email Phishing Recipe

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

Preheat your email system with some basic email protection controls, building a foundation for your dish. Mix in MFA for remote access, protecting against potential credential theft. Place in oven at high temp for incident response plan testing.

When finished baking sprinkle with additional tooling to provide next level protection to taste. Let cool several hours while providing the workforce training on reporting phishing attacks in the new system. Garnish with education on how digital signatures demonstrate authenticity of the sender.

Just like with any cookbook the recipes provide the basic ingredients to making a meal. It does not instruct you how to cook, instruct you on what recipes to use or limit your ability for substitutions. **The skill of the cook is what makes the dish!**

42

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**…

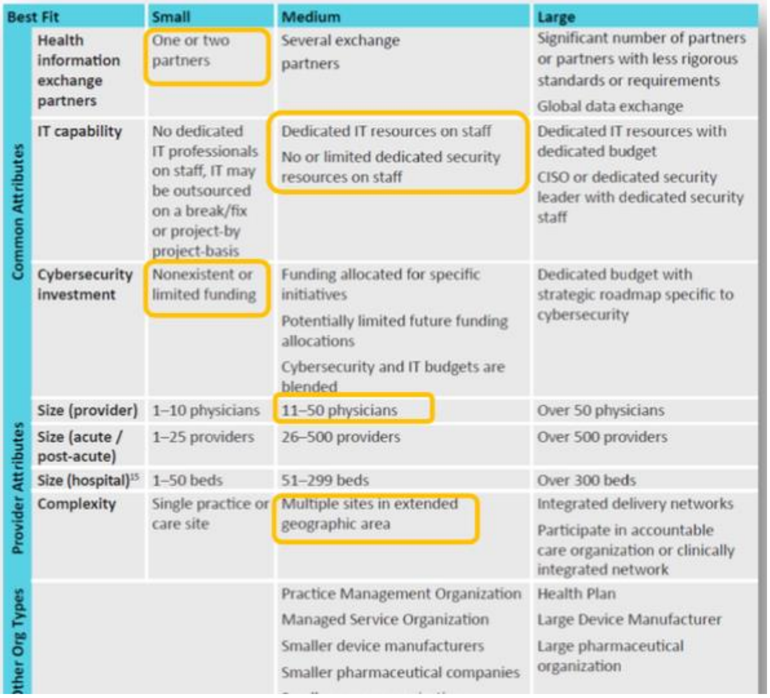
- A new regulation
- An expectation of minimum baseline practices to be implemented in all organizations
- The definition of "reasonable security measures" in the legal system
- An exhaustive evaluation of all methods and manners to manage the threats identified
  - You might have other practices in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

What Size is My Organization?

Factors Determining Size:

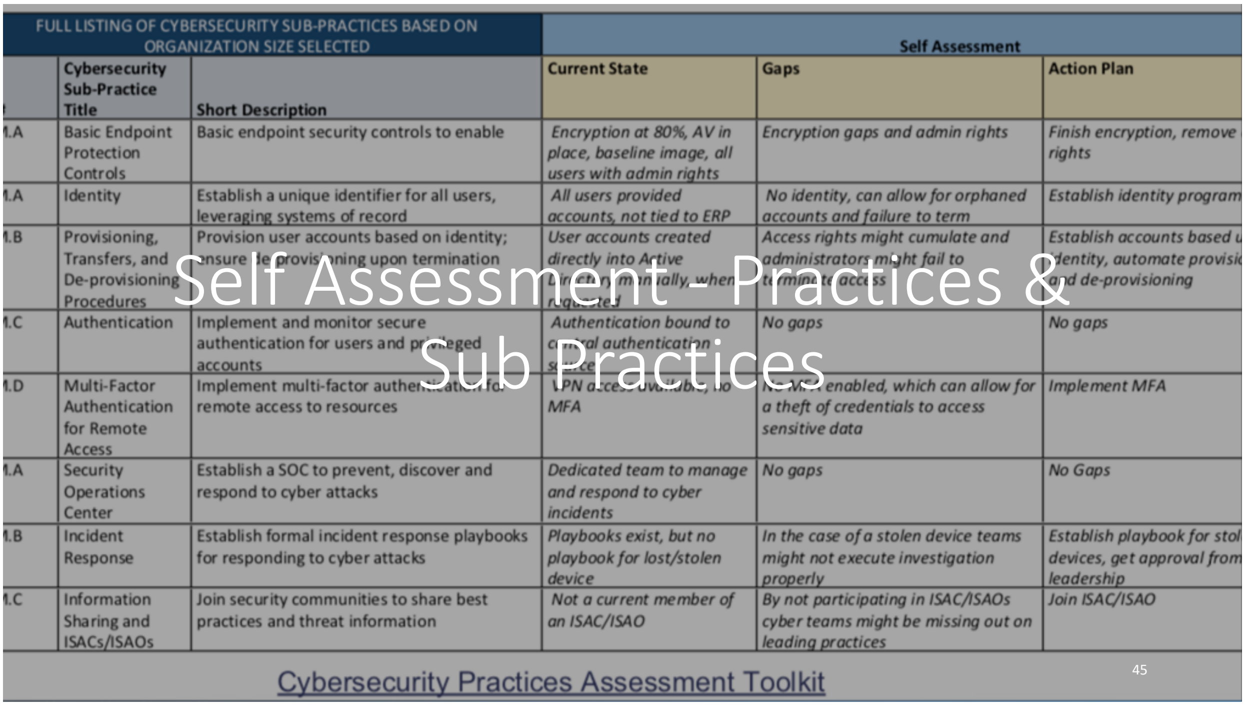
- Health Information Exchanges
- IT Capability
- Cybersecurity Investment
- Size (provider)
- Size (acute/post-acute)
- Size (hospital)
- Complexity

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	Health Plan Large Device Manufacturer Large pharmaceutical organization

Self Assessment - Practices & Sub Practices

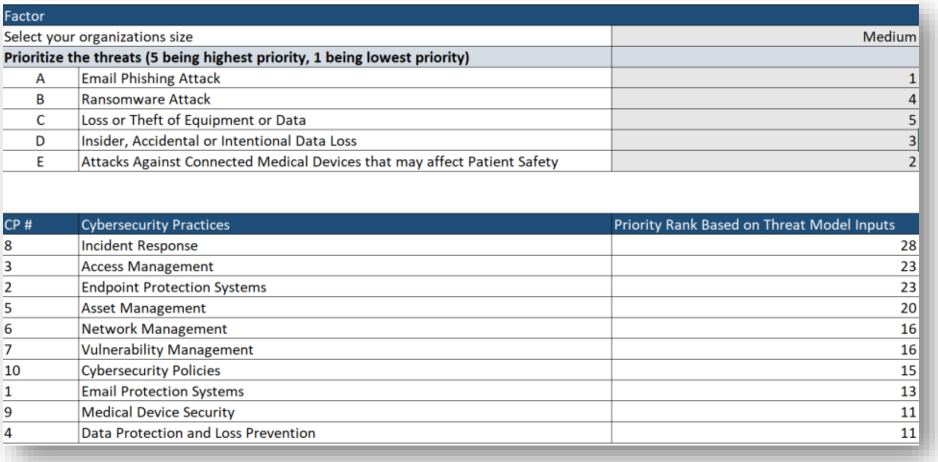


FULL LISTING OF CYBERSECURITY SUB-PRACTICES BASED ON ORGANIZATION SIZE SELECTED			Self Assessment		
	Cybersecurity Sub-Practice Title	Short Description	Current State	Gaps	Action Plan
1.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	*Encryption at 80%, AV in place, baseline image, all users with admin rights*	*Encryption gaps and admin rights*	*Finish encryption, remove rights*
1.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*
1.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 u identity, automate provisic and de-provisioning*
1.C	Authentication	Implement and monitor secure authentication for users and privileged accounts	*Authentication bound to central authentication source*	*No gaps*	*No gaps*
1.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*
1.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*
1.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 stol devices, get approval from leadership*
1.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*

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

Templates

- Glossary of Terms
- NIST Cybersecurity Framework Crosswalk
- Assessment Methodology
- Toolkits

- Examples
  - Portable devices policy
  - Incident response policy
  - Access control procedure
  - Security incident report sample
  - Onboarding and Offboarding policy
  - TECFA Do's and Don'ts

47

47

405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! These 5 threat posters were created in support of Cybersecurity Awareness Month in October 2019 to be used in hospitals, doctor's offices and even in email threads!

How Are the Phish Biting Today?
Protect Connected Medical Devices
...ed Your Workspace Today?
See Something Say Something
Don't Let Ransomware Hold your Data Hostage
HOSPITAL

THE 405(d) POST

A Word From the Task Group

A Simple Model to Discuss Cyber Risks with Executives

In This Issue, We're Covering:

- A Simple Model to Discuss Cyber Risks with Executives By: Erik Decker, Task Group Member
- HICP in the Spotlight: Two-Factor Authentication
- 405(d) Announcements
- Happening Around Us: New FDA Warning, Oregon Phishing Attack, Ohio Ransomware Attack
- Other HHS News

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters and Spotlight Webinars to increase cybersecurity awareness. They also present on new emerging cybersecurity news and topics, to include highlighting the HICP Publication!

405(d) Social Media

The 405(d) Program is now live on Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

Request materials – cisa405d@hhs.gov

48

HHS 405(d) Group

- Collaboration center for HHS Office of the CIO
- HICP
  - Update current information
  - Add additional detail
- 405(d) Communications
  - Videos
  - Newsletter
  - How to guides (S,M,L)
- Executive Leadership's role
- Impactful metrics

Resources and Solutions

HICP Documents - https://cybertygr.com/resource.html or https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

Business Case for Medical Device Security

Free Medical Device Security ROI
https://cybertygr.com/connectedmd.html

Automatically Document Security Efforts
Governance, Risk & Compliance Software
https://cybertygr.com/hipaamanage.html

Ty Greenhalgh – Ty@CyberTygr.com

Thank you