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

- 20-years plus in health information management
- Health ISAC-Board Member
- Certified Information Systems Security Professional (CISSP) ISC²
- 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) ISC²
- 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

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

“Bummer of a birthmark, Hal.”
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

Healthcare Breach and Incident Volumes

Total HIPAA Penalty Amounts by Year

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
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 Outdated or insufficient training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.”

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

March 06, 2019 | Rick Weber
NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY
CYBERSECURITY FRAMEWORK

Goal
- Manage risk tolerance
- Maturity level targeting
- Implement controls & safeguards

HHS supports crosswalk
- HIPAA crosswalk
  In development now
  New Functions: Control & Inform
  Likelihood, Problematic Data Action, Impact
  Alignment on Tiers
  Partial, Risk Informed, Repeatable, Adaptive

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.

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
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

Who is Participating
The 405(d) Task Group is not owned 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 aimed 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 in focus groups of 9-15 participants via roundtable discussions. A total of 123 took part in the pretesting effort.

Release

Future

Pretest

Start 405(d)

Our Mandate
- Become the leading collaboration center for developing healthcare cybersecurity focused resources
- 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.phe.gov/405d

https://www.cybertygr.com/resource
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

<table>
<thead>
<tr>
<th>Practice</th>
<th>Sub-Practice</th>
<th>To Consider</th>
<th>NIST Reference</th>
</tr>
</thead>
</table>
| Email 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 senders | 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 FRAMEWORK 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

<table>
<thead>
<tr>
<th>Data that may be affected</th>
<th>Passwords, PHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium Sub-Practices</td>
<td>1.M.A Basic E-mail Protection Controls</td>
</tr>
<tr>
<td></td>
<td>1.M.B Multifactor Authentication for Remote Access</td>
</tr>
<tr>
<td></td>
<td>1.M.C E-mail Encryption</td>
</tr>
<tr>
<td></td>
<td>1.M.D Workforce Education</td>
</tr>
<tr>
<td>Large Sub-Practices</td>
<td>1.L.A Advanced and Next-Generation Tooling</td>
</tr>
<tr>
<td></td>
<td>1.L.B Digital Signatures</td>
</tr>
<tr>
<td></td>
<td>1.L.C Analytics Driven Education</td>
</tr>
</tbody>
</table>

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
### Self Assessment - Practices & Sub Practices

<table>
<thead>
<tr>
<th>Type</th>
<th>Cybersecurity</th>
<th>Sub-Practice Title</th>
<th>Short Description</th>
<th>Current State</th>
<th>Gaps</th>
<th>Self Assessment</th>
<th>Action Plan</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.M.A</td>
<td>Basic Endpoint Controls</td>
<td>Basic endpoint security controls to enable prevention, deterrence and response for threats</td>
<td>Encryption of BER, AV in place, baseline image, all users with admin rights</td>
<td>Encryption gaps and admin rights</td>
<td>Finish encryption, remove admin rights</td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.M.A</td>
<td>Identity</td>
<td>Establish a unique identifier for all users, leveraging systems of record</td>
<td>All users provided accounts, not tied to EAP</td>
<td>No identity, can allow for orphaned accounts and failure to term</td>
<td>Establish identity program</td>
<td>Mfr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.M.B</td>
<td>Privileging, Transition, and De-privileging Procedures</td>
<td>Privilege user accounts based on identity, ensure de-privileging upon termination</td>
<td>User accounts created directly into Active Directory manually, when terminated</td>
<td>Access rights might cumulative and administration might fail to terminate access</td>
<td>Establish accounts based upon identity, automate privileging and de-privileging</td>
<td>Mfr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.M.C</td>
<td>Authentication</td>
<td>Implement and maintain secure authentication for users and privileged accounts</td>
<td>Authorization based on control authentication access</td>
<td>No gaps</td>
<td>No gaps</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.M.D</td>
<td>Multi-Factor Authentication for Remote Access</td>
<td>Implement multi-factor authentication for remote access to resources</td>
<td>MFA access available, no MFA</td>
<td>No MFA enabled, which can allow for a host of vulnerabilities to access sensitive data</td>
<td>Implement MFA</td>
<td>Mfr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.M.A</td>
<td>Security Operations Center</td>
<td>Establish a SOC to prevent, discover and respond to cyber attacks</td>
<td>Dedicated team to manage and respond to cyber incidents</td>
<td>No gaps</td>
<td>No Gaps</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.M.B</td>
<td>Incident Response</td>
<td>Establish formal incident response playbook for responding to cyber attacks</td>
<td>Phases exist, but no playbook for local incident device</td>
<td>In the case of a stolen device teams might not execute investigation properly</td>
<td>Establish playbook for stolen devices, get approval from leadership</td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.M.C</td>
<td>Information Sharing and IM/SAIAO</td>
<td>Join security communities to share best practices and threat information</td>
<td>Not a current member of an IM/SAIAO</td>
<td>By not participating in IM/SAIAO cyber teams might be missing out on leading practices</td>
<td>Join IM/SAIAO</td>
<td>High</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cybersecurity Practices Assessment Toolkit

### Prioritization Tool

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

#### Factor

<table>
<thead>
<tr>
<th>Select your organization’s size</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prioritize the threats (1 being highest priority, 1 being lowest priority)</td>
<td></td>
</tr>
<tr>
<td>A Email Phishing Attack</td>
<td>1</td>
</tr>
<tr>
<td>B Ransomware Attack</td>
<td>4</td>
</tr>
<tr>
<td>C Loss or Theft of Equipment or Data</td>
<td>5</td>
</tr>
<tr>
<td>D Insider, Accidental or Intentional Data Loss</td>
<td>3</td>
</tr>
<tr>
<td>E Attacks Against Connected Medical Devices that may affect Patient Safety</td>
<td>2</td>
</tr>
</tbody>
</table>

#### CP # Cybersecurity Practices

<table>
<thead>
<tr>
<th>Priority Rank Based on Threat Model Inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Incident Response</td>
</tr>
<tr>
<td>3 Access Management</td>
</tr>
<tr>
<td>2 Endpoint Protection Systems</td>
</tr>
<tr>
<td>5 Asset Management</td>
</tr>
<tr>
<td>6 Network Management</td>
</tr>
<tr>
<td>7 Vulnerability Management</td>
</tr>
<tr>
<td>10 Cybersecurity Policies</td>
</tr>
<tr>
<td>1 Email Protection Systems</td>
</tr>
<tr>
<td>9 Medical Device Security</td>
</tr>
<tr>
<td>4 Data Protection and Loss Prevention</td>
</tr>
</tbody>
</table>
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 (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.

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.

THE COOK MAKES THE DISH

The publication does not:
- Instruct you how to cook
- Instruct you on what recipes to use
- Limit your ability for substitutions

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
Thank you for joining us

Contact 405(d):
CISA405d@hhs.gov

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

Questions