THE 405(d) POST

Volume 2

A Word From the Task Group

Finding the Right Balance for Your Organization: The Difference between Base HIPAA Compliance and Cybersecurity Best Practices

By: Lee Barrett, 405(d) Task Group Member

In This Issue

When organizations are making decisions about implementing privacy and security controls, whether in preparation for EHNAC Accreditation, HITRUST, other certifications, or simply HIPAA/HITECH compliance, the area of cybersecurity best practices can cause confusion.

The two most important things to know when implementing healthcare cybersecurity policies and procedures in your organization are:

1 – Your Organization

2 – What is required versus what is recommended as a Best Practice?

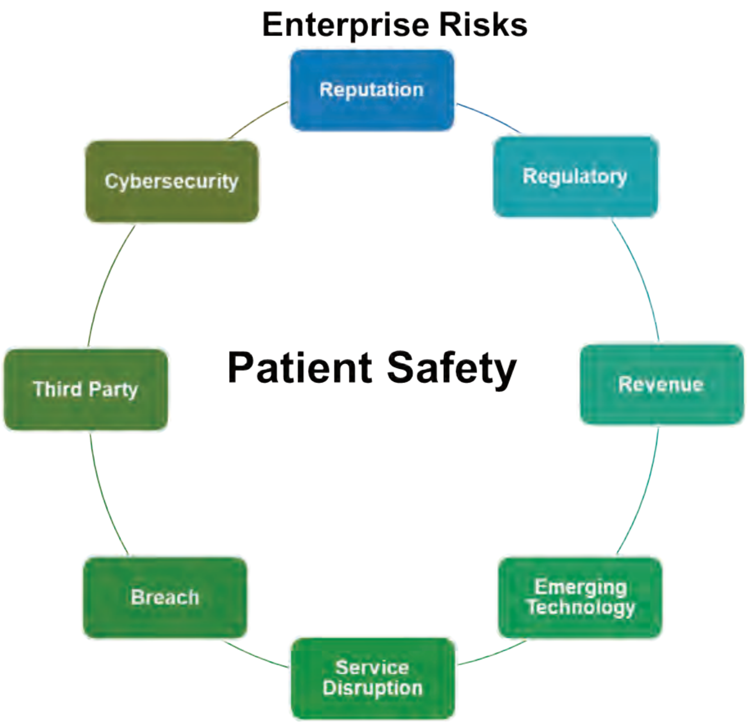
Know Your Organization

Understanding your organization's compliance stance, risk tolerance, the people who implement the work, and the technology and tools aiding them, are recommendations to assuring successful compliance with privacy and security. These requirements include understanding the landscape of your organization from the perspective of workforce members. Consider the following:

- *Do workforce members come on-site to conduct business or are they allowed to work virtually or in alternative locations?*
- *How is your business subject to HIPAA as a Covered Entity? A Hybrid Entity? A Business Associate?*
- *What is the status of current written policies, procedures, and risk tolerance as they relate to the administrative, physical, and technical aspects of the data you handle?*
- *Is your data classified (Protected Health Information versus Personally Identified Data or additional categories which include, but are not limited to confidential business information)?*
- *Do you conduct ongoing threat and risk analysis? What kind of ongoing monitoring occurs?*
- *Can data be wiped technically from any mobile devices with PHI at a moment's notice?*
- *Can you provide a current inventory/asset list of all hardware and software?*
- *Do you know who your downstream business partner(s) are, how they handle the data you entrust to them, and whether or not they conduct ongoing risk analysis to safeguard the PHI?*
- *Is there a process to constantly stay current with standards and best practice recommendations such as the NIST Cybersecurity recommendations or the 405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients document?*

Know what is required versus Recommended as a Best Practice

Organizations subject to regulatory requirements, such as the HIPAA Rules, must implement minimum standards to safeguard their data. Organizations may want to consider implementing additional measures and industry best practices including the 405(d) *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* document which outlines the five major threats facing the healthcare industry and ten practices that can be used to mitigate them. NIST or other Standards Development Organizations, which offer educational materials on privacy and security topics, can also be used to supplement regulations.



When considering whether to implement these best practice recommendations, staff must balance the risk of not implementing the best practice against the cost and/or complexity of implementing it for your organization. There are many factors to consider for every organization, including risk tolerance and exposure, scale, data and PHI flow, business partners etc. Be sure to document the rationale as to why a standard or best practice is or is not applicable to include in your policies and implementation practices. This type of information is important to include in your risk analysis to assure reconsideration in the future as your organization evolves and/or technology changes. Cybersecurity risks are enterprise risks. These risks can affect every aspect of your organization including your reputation. The most important risk is **patient safety,** which is the corner stone of every organization. Determining the appropriate balance between which best practices to implement and what are required by regulation for the data you handle is an important aspect of the cybersecurity assessment and implementation process. The criticality of properly assessing needs, requirements, applicable standards, need for third party services, and which cybersecurity best practices to employ are all factors in determining your strategy and tactics for your organization.

HICP Spotlight

Ransomware

Ransomware is a consistent and increasing threat to our industry; just last month three hospitals in Alabama were shut down due to 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.**

Real World Scenario:

Through an e-mail that appears to have originated from a credit card company, a user is directed to a fake website and tricked into downloading a security update. The so-called security update is a malicious program designed to find and encrypt data, rendering them inaccessible. The program then instructs the user to pay a ransom to unlock or unencrypt the data. In the meantime, the doctor's office is unable to access important patient information and deliver care until they have access to their computer systems.

What you can do about it:

Did you know, 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.

Located in *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* are ten practices any organization can use to mitigate cyber threats. Each of the ten practices address Ransomware from its many angles.

To learn more about Ransomware and the ten practices access *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients here!*

Also check out more resources HHS offers for Ransomware in the HHS Resources Section!

18%

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

Healthcare ransomware attacks will increase

x4 by 2020

Happening Around Us

Three Hospitals in Alabama Forced to Turn Patients Away after Ransomware Attack

CNN reports three hospitals in Alabama remained closed from October 2nd to October 11th to all but the most critical new patients due to a ransomware attack that disrupted medical care. Staff at the three hospitals had to use paper instead of digital records when providing care. While federal authorities worked to restore DCH computer systems, any non-critical new patients were sent to other hospitals, and local ambulances were directed to take patients to other facilities instead. After the incident the hospital network reported the attack to law enforcement and hired independent IT security and forensics experts to work on restoring the computer systems. Unfortunately, the hospital network was faced with the choice of paying the ransom in order to restore functionality of the system.[1] The Federal Bureau of Investigation discourages organizations from paying ransoms as there is no guarantee full restoration will occur. This is every hospital's worst nightmare and it is further evidence that Cyber Safety is Patient Safety. To learn more about Ransomware and the ten best practices to mitigate this threat access Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients here!

405(d) Events and Announcements!

National Critical Infrastructure Security and Resilience Month Toolkit now available!

405(d) Spotlight Webinar: Ransomware – December 11th at 1pm EST

Happy Birthday HICP! December 28th

***For information on the Spotlight Webinar or to receive the NCISRM Toolkit email us at cisa405d@hhs.gov!**

Confidence in Cyber Resilience Decreases, as Cyber Risk Prioritization is on the rise

HealthITSecurity reports business leaders are increasingly recognizing the impact cyber risks pose to their enterprise wide operations, but a Marsh-Microsoft report shows confidence in the ability to detect cyber threats is declining. The reports surveyed business leaders and found 18 percent of respondents said they had no confidence in understanding and assessing cyber risks and 19% had no confidence in preventing cyber threats, up from 12 percent since 2017. Also, overall, 43% of respondents said they have no confidence in their ability to prevent cyber threats from at least one of their third-party partners. As cybersecurity moves from being an IT-related issue to an enterprise wide issue it is increasingly important for security leaders to begin shifting the needle to become more effective.[2] To learn more and share information about cybersecurity to different parts of your organization, check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.[2]

Healthcare Cybersecurity Market to Reach 27.10 Billion by 2026

Yahoo Finance reports the global healthcare cybersecurity market was valued at USD 7.66 billion in 2018 and is expected to reach USD 27.10 billion by 2026, at a compound annual growth rate of 16.8%. The healthcare industry progressively depends on technology connected to the internet from patient records and lab results, to radiology equipment and hospital elevators. It has proven to be lucrative for patient care, as it predominantly facilitates data integration, patient engagement, and clinical support. Those technologies are often vulnerable to cyberattacks, which can siphon off patient data, hijack drug infusion devices to mine cryptocurrency, or shut down an entire hospital until a ransom is paid. Cybersecurity in healthcare situations is not easy and will require cooperation from everyone, including doctors, nurses, IT professionals, and manufacturers.[3] To learn more about the five major threats facing the healthcare industry and ten best practices you can use to mitigate them, check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.

HHS Ransomware Resources

HC3 Sodinokibi Ransomware Whitepaper

https://content.govdelivery.com/attachments/USDHSCIKR/2019/09/12/file_attachments/1284515/Sodinokibi-Aggressive%20Ransomwware_Whitepaper.pdf

HHS HC3 Briefing: Ransomware Threat to State and Local Governments

https://content.govdelivery.com/attachments/USDHSCIKR/2019/06/04/file_attachments/1224512/TLPWHITE_UNCLASSIFIED_20190530_State%20Local%20Gov%20Ransomware.pdf

HHS Office For Civil Rights Ransomware Guidance

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

HHS Office for Civil Rights Cyber Attack Check-List and Response Infographic

https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf

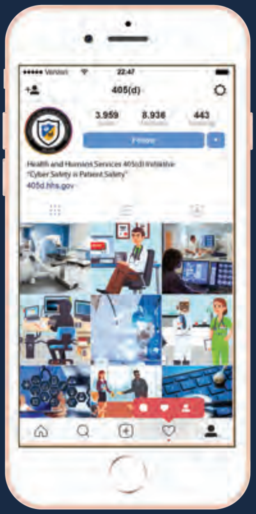
https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif

Coming Soon: 405(d) Social Media!

The 405(d) initiative will be taking cybersecurity awareness to Twitter, Facebook, and Instagram! Be sure to check us out starting early 2020!

Twitter & Instagram: @ask405d

Facebook: facebook.com/ask405d


405(d)
3,959
8,936
443
Follow
Health and Human Services 405(d) Initiative
"Cyber Safety is Patient Safety"
405d.hhs.gov

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Contact Us!

www.phe.gov/405d

CISA405d@hhs.gov

[1] https://www.cnn.com/2019/10/11/us/alabama-hospital-ransomware-attack/index.html

[2] https://healthitsecurity.com/news/cyber-risk-prioritization-increasing-as-confidence-in-resilience-wanes

[3] https://finance.yahoo.com/news/healthcare-cybersecurity-market-reach-usd-142124737.html

*DISCLAIMER: This newsletter is for information purposes only and aims to broaden awareness and align healthcare security approaches. The news articles represented in this newsletter are chosen at random to foster awareness and are not in promotion of any news organization. The "A Word from the Task Group" is written by a different 405(d) Task Group Member each issue and does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this newsletter.