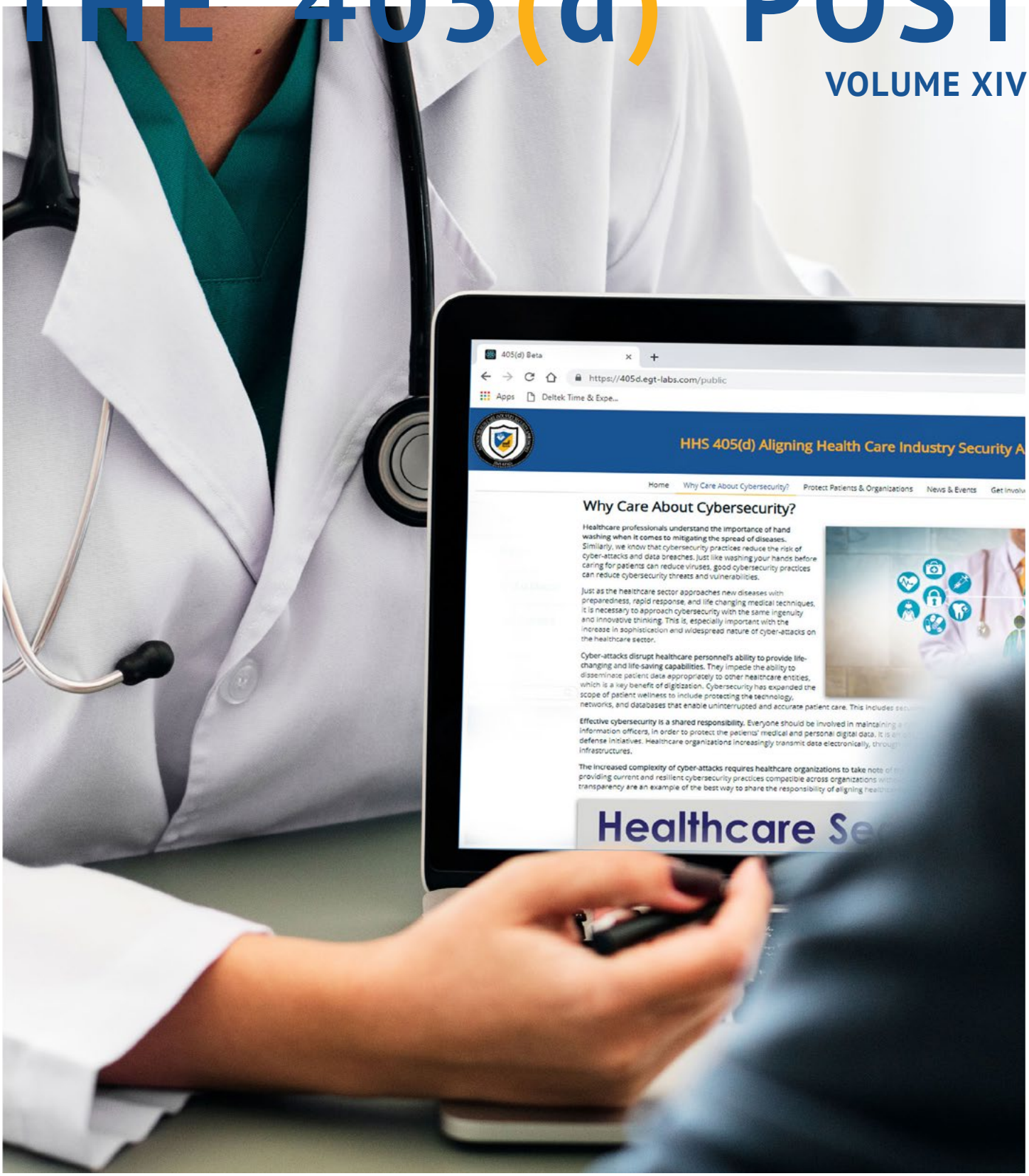
THE 405(d) POST

VOLUME XIV



HHS 405(d)
Aligning Health Care
Industry Security Approaches

A Word from the Task Group

Using Nested Encryption as a Process for Protected Data Batch Transfer Continuity

By Gary Haney, 405(d) Task Group member

Covered Entities and Business Associates have the responsibility to guarantee the safety and security of protected data both at-rest and in-transit. Examples of protected data include: Protected Health Information (PHI), Payment Card Information (PCI), Personal Financial Information (PFI), and Personally Identifiable Information (PII). Failure to protect this data at-rest and/or in-transit results in a loss of "safe harbor" and could potentially result in the exposure of protected data. Some laws and regulations, such as HIPAA, allow for "safe harbor" from breach notification obligations for data that is appropriately secured when transmitted over a public network. The following actionable steps can help you apply nested encryption practices to better avoid these risks and protect your patients and organization.

In-Transit Nested Encryption

The encryption of Transmission Control Protocol/Internet Protocol (TCP/IP) traffic has been used for several years and the protocols have evolved from Secure Sockets Layer (SSL) to Transport Layer Security (TLS) over time. However, all versions of SSL currently have software vulnerabilities. Earlier versions of TLS also have similar software issues that make using just transport-layer encryption no longer acceptable.

Loss of "safe harbor" means that protected data should no longer be stored or transmitted using software with known vulnerabilities. Yet, we must still communicate with Business Associates for the treatment, payment, and/or operation of healthcare practices.

If we view encryption as a means of putting a secure envelope around our protected data, nested encryption is simply a secure envelope within a secure envelope. Using a nested encryption method for sending batch-oriented transfers of protected data provides Covered Entities and Business Associates with a process to continue to transfer protected data. This process can be followed even if software vulnerabilities are exposed within either the at-rest encryption protocol or the in-transit encryption protocol.

Loss of "safe harbor" would only occur if there are un-mitigated software vulnerabilities in both encryption protocols at the same time.

Choose Your First Envelope

Nested encryption makes use of both at-rest and in-transit encryption technologies. The first encryption envelope is usually the at-rest encryption protocol and is usually some form of public/private key technology.

What types of data can be encrypted with an at-rest technology? Basically, any flat file or group of files. A report on patient outstanding accounts receivable (AR) being sent to your Revenue Cycle vendor, a batch file containing Health Level 7 (HL7) transactions for a Business Associate, or even Picture Archiving and Communications System (PACS) images with Digital Imaging and Communications in Medicine (DICOM) data can all be encrypted with an at-rest technology.

When using nested encryption, it is important to ensure that the exchange of the public-key (or the decryption password) with other Covered Entities or Business Associates occur via a separate secured communication channel. This will maintain the secrecy of the data.

The output of this initial encryption process is an encrypted flat-file (potentially containing multiple files when unencrypted) that can be transmitted to other Covered Entities or Business Associates using an encrypted in-transit communication protocol.

Choose Your Second Envelope

This second envelope is typically done within the TCP/IP protocol and is typically using TLS1.2 or higher. However, the other forms of in-transit encryption could potentially be used if a successful TLS1.2 connection cannot be negotiated.

In this case, using a secure file transport protocol (FTP), such as Secure FTP (SFTP) could become the second envelope of protection.

When using TLS, it is important to understand how your TLS protocol is configured when a connection to remote sites is set up and negotiated. Some TLS settings allow the encryption layer to be negotiated at lower levels than TLS1.2 or higher and could invalidate establishing a safe method of in-transit security. It is highly advised that your servers be configured to only accept TLS 1.2 and higher levels of encryption.

As an example, on Windows Internet Information Services (IIS) servers, in the Internet Options window on the Advanced tab, under Settings, scroll down to the Security section. In the Security section, locate the "Use SSL" and "Use TLS" options. Uncheck "Use SSL 3.0" and "Use SSL 2.0". If they are not already selected, uncheck "Use TLS 1.0" and "Use TLS 1.1". Ensure the "Use TLS 1.2" option is the only one checked.

Please check with your vendor to ensure that your software will support TLS version 1.2. If they will not support TLS 1.2, then you may want to consider using an alternate in-transit encryption protocol such as Secure FTP in place of an older version of TLS in order to maintain secure at-rest and in-transit protocols.

Communicate Your Change

Before you start using nested encryption for any batch transmissions of any protected data, be sure to communicate! If needed, negotiate with other Covered Entities and Business Associates to determine the best processes to use to enable nested encryption with these remote partners.

Conclusion

The importance of maintaining "safe harbor" is an essential part of maintaining appropriate protections required for the safety and security of the protected data with which we have been entrusted. Hopefully this article has provided guidance and direction surrounding why nested encryption is needed to ensure business continuity and prevent the loss of "safe harbor" for transmission of protected data over a public network.

HICP in the Spotlight
2021 Year in Review

Throughout 2021, the U.S. Department of Health and Human Services (HHS) 405(d) Program executed various strategic engagements and communication campaigns in an effort to continue the mission and vision of the program: "Aligning Healthcare and Security Approaches." Additionally, the program helped grow the reach of the task group by adding an additional wave and setting up the Task Group Ambassador program. Task Group Members also worked diligently on new 405(d) publications regarding Enterprise Risk Management and Tactical Crisis Response, adding to the 405(d) library of cybersecurity resources for the Healthcare and Public Health sector. Overall, the program continues to build upon the work completed in previous years and has refined its approaches to promote the message that **Cyber Safety is Patient Safety.**

ENGAGEMENT

6 Total Spotlight Webinars

800+ Total Spotlight Webinar Attendees

27 Total Products Released

12 Total Speaking Events

SOCIAL MEDIA

Across Linkedin, Twitter, Facebook, and Instagram:

384 Total Posts

84,461 impressions

80% follower growth from beginning of 2021

HICP in the Spotlight
2021 Year in Review

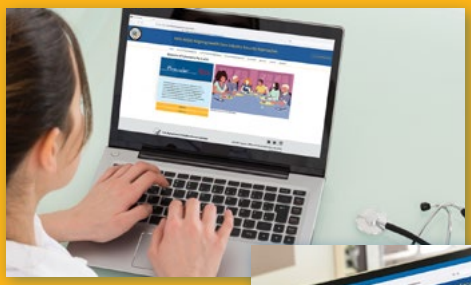
405(d) SBARs and the Tiger Team

In order to help the HPH sector better respond to cybersecurity events, the 405(d) Program established a Tiger Team, which consists of 405(d) Task Group members that discuss time-sensitive cybersecurity alerts and events that are relevant to the HPH sector. The Tiger team develops an **SBAR Situation, Background, Assessment, and Recommendation** product that is tailored specifically for the HPH sector. The Recommendations are all pulled from the HICP Publication. This is a **new** 405(d) product and in 2021, we released **three** of these quick turnaround reports.

Kaseya VSA Supply Chain Ransomware Attack SBAR

VMware Critical Patch Update SBAR

Log4j SBAR

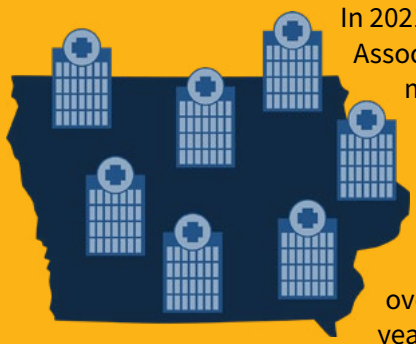


161,255
website hits in December

405(d) Website

On December 1st, through OCIO and OIS, the 405(d) Program launched the official HHS 405(d) Program website—405d.hhs.gov. Through this new website, which was developed in partnership with the 405(d) Task Group, the 405(d) Program will provide the HPH sector useful, impactful, and industry-tested resources, products, videos, and tools that help raise awareness and provide vetted cybersecurity practices. In turn, we should see a drive in behavioral change and move toward consistency in mitigating the most relevant cybersecurity threats to the sector. In its first full month in December, the 405(d) Program's new website received a total of **161,255 hits.**

State-Wide Training with HICP



In 2021, the Iowa Primary Care Association provided their members with cybersecurity training based on the 405(d) HICP publication. The training sessions focused on all ten practices and took place over the course of an entire year. This engagement reached small practices and exemplifies the best use of utilizing HICP within small organizations and an example of how associations can help use or increase the adoption of HICP.

October 405(d) Spotlight Webinar

The 405(d) October Spotlight Webinar held on October 5th saw an audience of 205+ attendees, a new high for the program's bi-monthly recurring event. This webinar consisted of a new format which included a representative from a healthcare network whose organization experienced a cyber attack in 2020, and federal representatives from Cybersecurity & Infrastructure Security Agency (CISA), Federal Bureau of Investigations (FBI), and HHS. Federal representatives provided feedback for viewers to help them learn about resources available. This event received rave reviews with members of the HPH sector calling it the **"gold standard"** and **"the best webinar they have ever attended."**

My Top 5 Reasons for Conducting Ongoing, Continuous Risk Analyses

By Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US, C|EH, NACD CERT, 405(d) Task Group Member

The 405(d) Chronicles is a platform for sharing firsthand insight, lessons learned, and perspectives from cybersecurity professionals in the field today.

The healthcare ecosystem has come a long way, and still has a long way to go, when it comes to risk analysis and risk management. More organizations are making an effort. Concurrently, the Office for Civil Rights (OCR) enforcement data for the last ten years has consistently shown that approximately nine out of ten organizations are not conducting the comprehensive, enterprise wide risk analyses and risk management explicitly called for in the HIPAA Security Rule.[1] Furthermore, we know there has been a bit of fibbing on those Meaningful Use Attestations, validating that risk analyses had been completed.

I am hopeful risk analyses will improve because of all the dedicated people working in privacy, security, compliance, and risk management. These thousands of hardworking professionals are committed to making it right and continue to garner the attention and support of their C-suites and boards. One of the things that continues to keep me awake at night is the lack of attention to the foundational requirement of conducting *ongoing, continuous risk analyses.* Cybersecurity is clearly becoming a patient safety issue. Therefore, we must make risk analysis part of the fabric of everything we do. Consider for a moment the lawsuit that has been filed against an Alabama hospital alleging that the medical team's inability to access critical fetal monitoring data and devices during a 2019 ransomware attack led to a baby's death.[2] The lawsuit specifically calls out the organization's failure to conduct risk analysis multiple times.[3]

The only viable path to a comprehensive Enterprise Cyber Risk Management (ECRM) program starts with ongoing, continuous risk analyses. The work of the 405(d) Task Group and upcoming publications of updated *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP) Technical Volumes underscores the importance of ongoing, continuous risk analyses for all covered entities, business associates, and hybrid organizations, large and small.

What Is Ongoing, Continuous Risk Analyses

Ongoing, continuous risk analyses means embracing the concept of security by design. It means building security into an organization's systems, product, or service development lifecycle. It also means understanding and staying ahead of the constantly changing cybersecurity landscape.

It does not mean checking that checklist one more time. It does not mean completing a compliance gap assessment. It does not mean once-and-done, annually, or periodically (whatever that means). It means risk analysis should be part of the fabric of the organization.

Hopefully, this brief article will motivate and inspire more diligence around this critical and foundational step to establish, implement, and mature an ECRM program.

Continued on next page.

My Top 5 Reasons for Conducting Ongoing, Continuous Risk Analyses

1. Stop Accruing More "ECRM Debt"

By "ECRM Debt", I am referring to dollars that should have been spent on managing cyber risk while the race to collect Meaningful Use incentive money was happening. Few dollars were allocated at the time and the cyber risk implications of those projects now need to be addressed. That ECRM Debt must be paid back and no more ECRM Debt should be accrued.

The best way to ensure no additional ECRM debt is incurred, is to withhold approval of any initiatives, projects, or programs involving healthcare data, systems, or devices- unless and until specific and appropriate funding has been designated for cyber risk management. In fact, NIST suggests that before a new system can be deployed, there should be an Authorization to Operate (ATO) or an Authorization to Use issued by senior management (Authorizing Official), contingent on the assessment of security and privacy risks.[4]

2. Be Prepared for More Disruptions

The COVID-19 pandemic is only one example of the type of disruption we face operating our healthcare organizations. The number one lesson is that disruption—in this case, driven by a pandemic—creates opportunities for new threat sources to appear. Disruption sets the stage for bad actors to exploit a significantly expanded attack surface. Remote work and re-engineered clinical and administrative workflows often used new information assets (e.g., home computers, Zoom, remote monitoring devices). These assets possessed vulnerabilities (i.e., unsecured home networks) that old and new threat sources could exploit; from these, a new set of risks were born. As a reminder, a risk exists when—and only when—an asset, threat, and vulnerability are present.

The reality is that disruption can originate from many sources, not just a pandemic. Socio-political, geopolitical, economic, technological, legal, and environmental factors all present opportunity for new risks to emerge.

Even without major disruptions, everything is changing! Organizations, people, assets, threats, vulnerabilities, controls, likelihood, impact, and, of course, cyber-attacks are continuously evolving. As former National Security Advisor McGeorge Bundy once observed, "If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds."[5] Among other good things that happen, continuous, ongoing risk analyses ensure we keep sorting our toothbrushes from our diamonds.

> "Risk analysis should be part of the fabric of the organization."

3. NIST Standards and Guidelines Call for a Continuous Approach

The National Institute of Standards and Technology (NIST) Cybersecurity Framework includes the Framework Core which "consists of five concurrent and **continuous** Functions—Identify, Protect, Detect, Respond, and Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk."[6]

The best overall risk management process an organization can follow is spelled out in "Managing Information Security Risk" (NIST Special Publication 800-39)[7] and comprises four basic steps, each of which informs the other steps in the process:

i. **Frame risk.** Establish the context for risk-based decisions and your overall approach to risk management.

ii. **Assess risk.** Identify your exposures via an enterprise-wide, comprehensive risk analysis.

iii. **Respond to risk.** Focus on making risk treatment decisions and executing risk treatment actions.

iv. **Monitor risk on an ongoing basis.** Conduct the risk management process continuously, which should include a feedback loop for process improvement. Risk management is not a once-and-done proposition.

Continuous, ongoing risk analyses facilitate alignment with the NIST Cybersecurity Framework, and the overall cyber risk management process established by NIST.

Continued on next page.

4. OCR Guidance Requires a Continuous, Ongoing Approach

OCR recommends conducting continuous risk analysis to identify when new safeguards are needed. OCR Guidance states, "A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation … Performing the risk analysis and adjusting risk management processes to address risks in a timely manner will allow the covered entity to reduce the associated risks to reasonable and appropriate levels."[8]

A great way to ensure compliance with the HIPAA Security Rule requirements for risk analysis and risk management is to conduct continuous, ongoing risk analyses.

5. Your Business is Ongoing and Continuous, So Should Your Risk Analyses

No matter what type of organization you represent in whatever industry, your vision, mission, strategy, values, and services are not static. They are ongoing and continuous. Your business planning processes are ongoing and continuous. Your organization is continuously monitoring and adapting to the changing internal and external environment by improving existing services and solutions or designing and providing new services and solutions.

Cybersecurity and cyber risk management are no longer simply a matter of compliance or data security; cyber risk is about patient safety and medical professional liability. It only stands to reason that your cybersecurity program evolves based on ongoing and continuous risk analyses. I highly recommend that you critically evaluate your current risk analysis processes against the standard that they should be ongoing and continuous.

Endnotes

1 Clearwater analysis of data publicly available at: Resolution Agreements and Civil Money Penalties. Health Information Privacy. U.S. Department of Health and Human Services. (n.d.) Accessed January 3, 2022. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

2 A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death. Kevin Poulsen, Robert McMillan, Melanie Evans. Sept. 30, 2021. Accessed January 3, 2022. https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

3 KIDD AMENDED COMPLIANT. June 4, 2020. Accessed January 3, 2022. https://www.documentcloud.org/documents/21072978-kidd-amended-complaint

4 Risk Management Framework for Information Systems and Organizations. NIST Special Publication 800-37, Revision 2. National Institute of Standards and Technology (NIST). December 2018. Accessed January 3, 2022. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

5 "Sorting diamonds from toothbrushes: New guide to protecting personal information." National Institute of Standards and Technology (NIST). January 13, 2009. Accessed January 3, 2022. https://www.nist.gov/news-events/news/2009/01/sorting-diamonds-toothbrushes-new-guide-protecting-personal-information

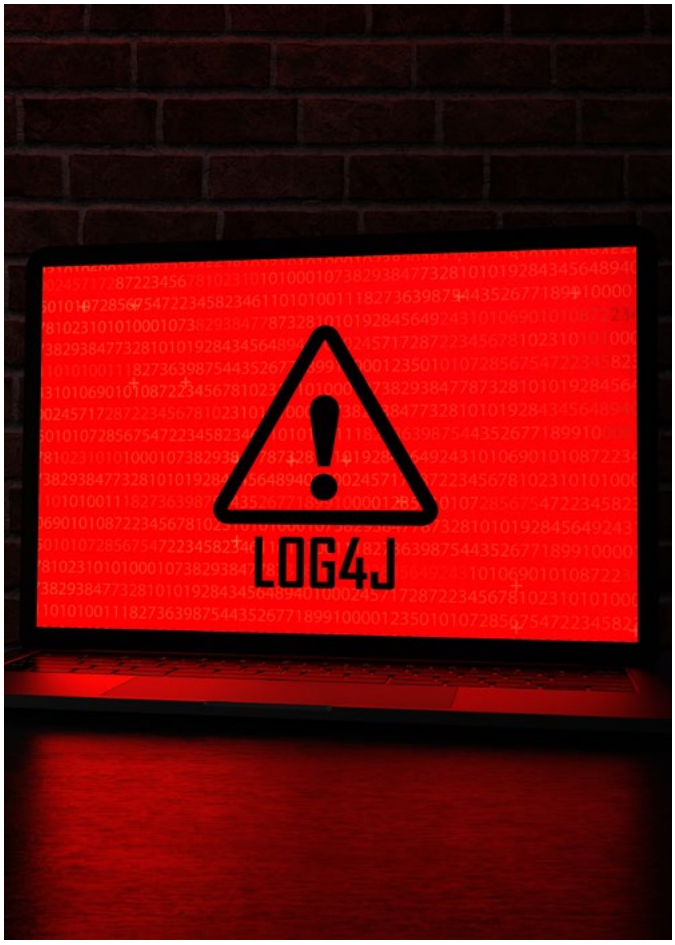
6 Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology (NIST). April 16, 2018. Accessed January 3, 2022. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

7 Managing Information Security Risk. NIST Special Publication 800-39. National Institute of Standards and Technology. March 2011. Accessed January 3, 2022. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

8 "Guidance on risk analysis requirements under the HIPAA Security Rule." OCR/HHS. July 14, 2010. Accessed January 3, 2022. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

Happening Around Us

The Internet Is on Fire: A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.



Wired reported that a vulnerability in a widely used logging library has become a full-blown security meltdown, affecting digital systems across the internet. Hackers are already attempting to exploit it, but even as fixes emerge, researchers warn that the flaw could have serious repercussions worldwide. The problem lies in Log4j, a ubiquitous, open source Apache logging framework that developers use to keep a record of activity within an application.

Read the full story, HERE.

Find recommendations from HICP and more information in the most recent 405(d) SBAR product, HERE.

Learn more mitigation practices with HICP, HERE.

PHI Breach, Data Exfiltration at Broward Health Impacts 1.3 Million

HealthITSecurity reported that Florida-based health system Broward Health provided notice of an October 2021 healthcare data breach that exposed protected health information (PHI) and resulted in data exfiltration. The breach has not been posted to the Office for Civil Rights (OCR) data breach portal yet, but a submission to the office of the Maine attorney general revealed that the breach impacted 1,357,879 individuals. An unauthorized bad actor gained access to Broward Health's network through the office of a third-party medical provider. The exposed information included Social Security numbers, phone numbers, birth dates, addresses, email addresses, financial account information, insurance information and account numbers, medical record numbers, and driver's license numbers.

Read the full story, HERE.

Learn how to protect your patients and organization from a data breach with HICP, HERE.

Missouri's Capital Region Computers, Phones Still Down Due to Hack

On December 28, 2021 Local Jefferson, Missouri ABC affiliate news station KHQA reported that the computer network and telephone systems at Capital Region Medical Center are still inoperative after a "cybersecurity incident" incapacitated them on December 17. According to spokesperson Lindsay Huhman, "the incident has impacted the network across the organization." At the time of the report, she said there is no timeline for a fix to be completed. Huhman added that the hospital has contacted the FBI and are cooperating with them fully in their investigation. The federal Cybersecurity and Infrastructure Security Agency (CISA) has also been notified.

Read the full story, HERE.

Learn how to protect your healthcare organizations and patients from cyber-attacks with HICP, HERE.

Other Federal Resources

HC3

- FIN12 as a Threat to Healthcare
- Log4j Update Sector Alert
- Hillrom Welch Allyn Cardiology Products Vulnerability Alert
- November 2021 Vulnerability Bulletin
- Log4j Scanner Alert

CISA

- Mitigating Log4Shell and Other Log4j-Related Vulnerabilities
- ICS Medical Advisory - Fresenius Kabi Agilia Connect Infusion System

OCR

- HHS Issues Guidance on HIPAA and Disclosures of Protected Health Information for Extreme Risk Protection Orders
- Five enforcement actions hold healthcare providers accountable for HIPAA Right of Access

Upcoming Events

Spotlight Webinar

Join us for our February Spotlight Webinar! Date and time to be announced soon.

About The 405(d) Post

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" and the "405(d) Chronicles" 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.

Need To Contact Us? Email us at cisa405d@hhs.gov

Follow us!

Facebook Twitter
Instagram LinkedIn

Visit our website at 405d.hhs.gov!