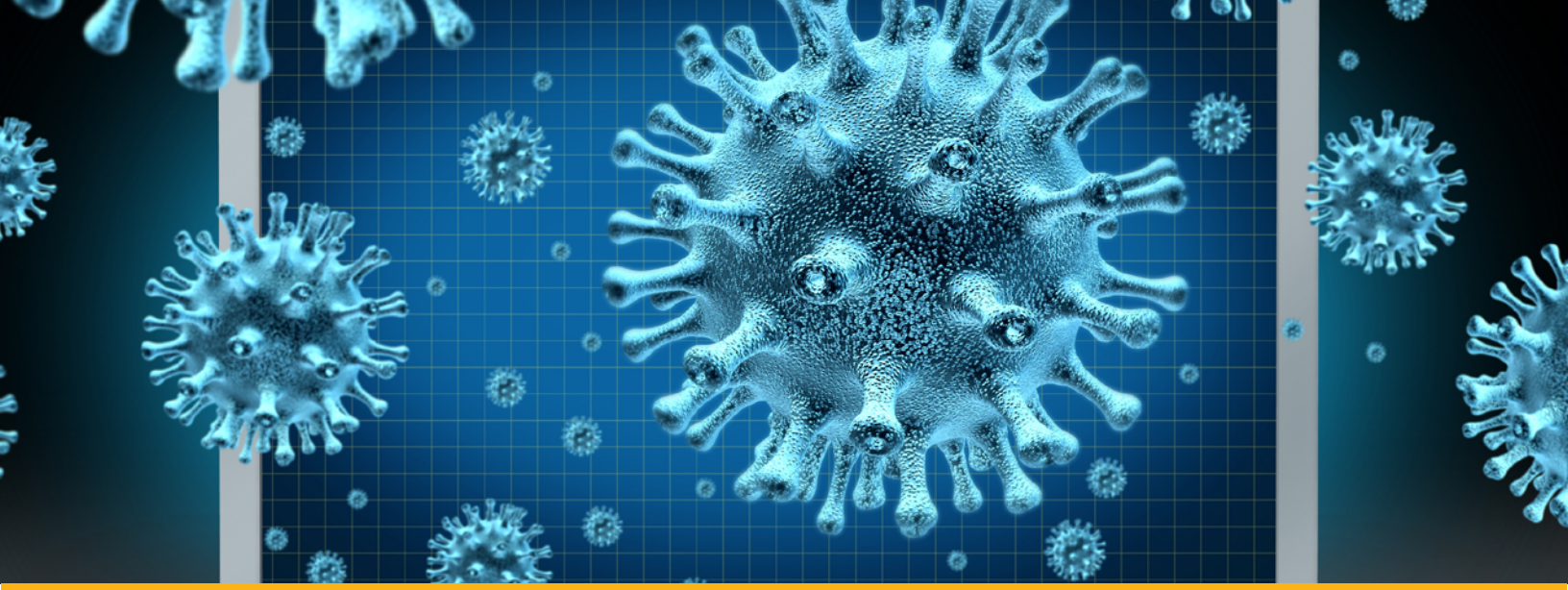
THE 405(d) POST

VOLUME IX

HHS 405(d)
Aligning Health Care
Industry Security Approaches



The 405(d) Task Group: A Year in Review

By Erik Decker, 405(d) Industry Co-Lead

Dear Colleagues,

Happy New Year from the 405(d) Program!

2020 was a trying year for our industry and not only did we experience unprecedented personal losses across the country, our industry also experienced an increase in cyber attacks which ultimately put all our patients in jeopardy. Our moment of crisis provided cyber criminals a pivotal opportunity to exploit the stresses on our healthcare system. According to Emisoft's ransomware report, healthcare experienced an increase in ransomware impacting hundreds of hospitals across the country[1]. The impacts of one particular attack was alarming: ambulances were rerouted, medical records were inaccessible, and even hundreds of staff were furloughed. Another example showed a university health system hit with ransomware forced to operate for over a month in Electronic Health Record (EHR) downtime. There are many more examples, which is why a continued dedication to cybersecurity in our health sector is paramount to care delivery and patient safety.

I want to personally thank the 405(d) Task Group and our greater 405(d) stakeholders for staying engaged throughout 2020, when it truly did matter most. Despite the difficulties each member of our Task Group faced in their day to day work, we continued to work diligently on new cybersecurity resources that will ultimately move the needle and create behavior change across our industry. I also witnessed our 405(d) stakeholders implementing the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication into their organizations and sharing their insights and results. This open dialog we continue to have as a program allows us to produce impactful products that are consensus-based practices, easy to use and implement, and universal across our sector.

As 2020 came to a close, we saw the biggest 405d(d) impact, when H. R. 7898 became law (and now officially referred to as Public Law 116-321[2]). The bill aims to amend the Health Information Technology for Economic and Clinical Health Act (HITECH) to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain oversight and enforcement determinations, and for other purposes.

The bill continues to state that "… the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015…" are under the definition of 'recognized security practices'.

1 https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/
2 https://www.congress.gov/bill/116th-congress/house-bill/7898/text/pl?r=2

This direct reference to 405(d) program and the resources produced under this public-private partnership is a major acknowledgement. I hope this achievement gives us all a renewed call to action to continue working together, providing our expertise and insight to create new products for our sector.

A Look to 2021

The 405(d) Program has an eventful 2021 planned for all our stakeholders. You will see new cyber awareness materials that you can utilize in your respective organizations to help train your staff about common cyber tactics, simple cyber resilience tips, and more. We will also continue our 405(d) Post to inform our stakeholders of new and timely cyber information, as well as our 405(d) Spotlight webinar which utilizes our Task Group to foster an environment of information sharing. You will also notice renewed activity on our Social Media Pages: Twitter, Facebook, LinkedIn, Instagram at @ask405d where you can access all our events, materials, and stay up to date with what's going on in all things cyber!

If you have not utilized this program and its resources in the past, I hope you will consider this new year as a great opportunity to start. There is no better moment in our industry's history to be engaged, informed or even over informed on how we can keep our patients safe from cyber threats.

Thank you,

Erik Decker

405(d) HICP in the Spotlight: Asset Management

Organizations manage IT assets using processes referred to collectively as IT asset management (ITAM). ITAM is critical to ensuring that the appropriate cyber hygiene controls are maintained across all assets in your organization. ITAM processes should be implemented for all endpoints, servers, and networking equipment. These processes enable organizations to understand their devices, with the best options to secure them. Although it can be difficult to implement and sustain ITAM processes, such processes should be part of daily IT operations. ITAM processes encompass the lifecycle of each IT asset, including procurement, deployment, maintenance, and decommissioning (i.e., replacement or disposal) of the device.

One practice for ITAM process is keeping an updated, accurate inventory. A complete and accurate inventory of your organization's IT assets facilitates the implementation of optimal security controls. This inventory can be conducted and maintained using a well-designed spreadsheet. Following inventory, an appropriate procurement and decommissioning process are also important to maintain accurate asset accounts. Following processes for each of these steps will ensure you always maintain an up to date field inventory.

Protecting our patients from cyber threats, even in these uncertain times, is key to keeping our healthcare systems running smoothly and securely. For more information on Asset Management, and other ways to protect your organization from cyber threats, check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication at www.phe.gov/405d.

405(d) Chronicles

By Donna Grindle, 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.

Early March 2020 seems like yesterday and also a lifetime ago. Direct patient care in small organizations had always centered around the office for the most part. Telehealth apps were being discussed and even tested out by some organizations but it wasn't a regular part of the patient care workflow. Then the Coronavirus (COVID-19) pandemic shutdown our world and overnight the shift to online patient care became an absolute, immediate necessity.

We were on the phone with many small organizations needing help on how to implement a secure solution to take care of their patients remotely. Oh, and implement it from scratch in 24 hours or less. Even after the Office of Civil Rights (OCR) enforcement discretion announcement relaxed requirements somewhat, many practices needed help to understand their options that the announcement provided. Those first three weeks were very challenging for everyone. The need to continue to provide care required a lot of moving parts and quick decision making from all over the industry.

Businesses everywhere were in a rush to develop work from home plans for as many team members as possible. IT providers were doing the best they could to get functionality up and running as machines were literally being pulled out of closets, dusted off and put into what we thought would be "temporary service". Personal devices were pushed into "temporary service" to fill the gaps.

Computers and tools like web cams were back-ordered for weeks. That "temporary service" was often much longer than originally expected. Most of us were using professional associations and connections with other businesses to find people and equipment needed. We worked together to figure it out as we went. Sharing resources and connections with others was a great way to manage the situation and to find out what was working and what wasn't.

As many have pointed out, it was a rapid digital transformation for us all.

Here we are a year later. Patients received care throughout the year that was 2020. Telehealth is very much a part of most small practice toolboxes now. Workflows that were adapted or added "on the fly" were adjusted and adapted into regular operation standards. IT providers are getting their hands around all the temporary remote configurations that now have become our standard operating environments.

When I listen to those small and medium organizations today describe where they are and decide where to go with all of these new options, one thing is for certain: we will not be returning to the old 2019 way of doing things. Sure, some of the things implemented didn't work well but others worked out to be even better than expected for everyone involved. Also, we are still trying to figure out the full impact this has had on our data, networks, and systems but any problems found will not represent a reason to go backwards, only to find a way to deal with it as we move forward.

Some things we learned I found interesting and unexpected. For example, some Electronic Health Records (EHRs) already in use within a practice had telehealth features available and practices used them immediately. It turned out for some practices, though, that they were better suited by using another third-party app that adapted better with their workflows or financial requirements. In other cases, the features built into their EHRs worked great, but they implemented a different third-party app for use in specific situations..

It is clear though, as always, that in healthcare there is no "one size fits all" for the best technology solutions to provide patient care. A lot of different variables have been at play in selecting the apps and technology that works best for each practice and their patients. Those responsible for securing these new work environments still have to adapt as everyone continues to evolve and slowly settles into whatever works best for them.

Here is what I believe we, as a sector, will have to consider and address moving forward

- **What will the Healthcare and Public Health (HPH) sector do about the folks that have gotten used to using technology for telehealth that doesn't meet Health Insurance Portability and Accountability Act (HIPAA) security standards due to the enforcement discretion guidelines?** In my organization I have suggested not using these options except when absolutely necessary but small providers all over the country have gotten used to using them now.
- **How does the HPH sector make it easier and more accessible for patients who may not have the skills, capabilities, or access to the technology required to participate in telehealth options?** A flip phone is in the hands of way more people than I realized! Rural areas have very limited access to high speed connections that support video calls.
- **How does the HPH sector better secure these organizations?** As their technology expanded so did their attack surface and, as we know, the threat landscape exploded. They haven't historically had access to technical and security specialists that protect larger organizations. Better guidance and tools will be essential to their success and continued digital transformation.
- **How much of what the HPH sector has learned been turned into preparations for the next pandemic or national crisis?** I believe every single business should do a review of what has worked, what hasn't worked and what they would like to do differently. Also I have found that updating our response plans with these lessons will helped me to be better prepared for the next one. Now, we know the unexpected must be seriously considered.

Throughout this national crisis one thing is for certain more than ever before, we must never forget that the job of those of us on the technology side of healthcare is to provide support and aid to those who actually provide care to patients. They need us to have the technology available and functioning in a manner that helps them efficiently care for patients while keeping them and their information safe at the same time.

Happening Around Us

Ransomware Trends into 2021

HealthITSecurity reports that ransomware was one of the healthcare sector's biggest cybersecurity threats in 2020 (much like in 2019), spotlighting the need for proactive measures. In 2020, the healthcare industry's resiliency was tested by its response to two national crises: a global pandemic and hackers taking advantage of a more vulnerable workforce. Ransomware was yet again the biggest cybersecurity threat, a further reminder of the need for proactive security measures. Ransomware's evolution is a sign of what's to come in 2021. Organizations continuing to hold a reactive cyber posture are at greatest risk. For those on guard, the multiple federal alerts that warned of a ransomware wave came as no surprise. Recently there has emerged a dominance of nation-state threat actors attempting to both disrupt care operations and to steal valuable data related to vaccines and treatments. It is expected that this surge which began in September 2020 will not die down. The need for more federal and state guidance on cybersecurity measures is paramount to saving lives through this pandemic.

If you are looking for more Ransomware protective measures, check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

https://healthitsecurity.com/features/biggest-healthcare-security-threats-ransomware-trends-into-2021

Attacks on VPNs and health industry headline 2021's biggest cyber risks

Security Magazine has reported that while Virtual Private Networks (VPNs) allow organizations to provide remote access, cybercriminals have figured out how to improve their own access. Alert hackers have devised new ways to exploit users and their organizations through virtual networks. In 2021 we will continue to see a boom in attacks on VPNs as legacy iterations and products are now more easily breached. While hackers love the challenge and reward of exploiting new technologies, VPNs frequently offer a familiar way to subvert common cyber precautions. Too often, VPN vendors are guilty of neglecting to patch vulnerabilities within their technology. Data-sensitive industries such as financial services, government, and healthcare are common users of VPNs that, without proper patching discipline, provide an open door for attackers to gain entrance to the networks. Over the past months, we have also seen rising VPN exploits due to stolen credentials and another dangerous reality—misconfigured clients. Difficult to detect, these are common pitfalls, especially as company clouds grow in complexity and resource span. To defend against VPN attacks, and to bring the most vulnerable attack vectors out of a hacker's reach, companies will need more sophisticated network access management. In order to exploit an entire organization, all a hacker needs to find is an employee with high access and low security hygiene.

To learn more about Access Management and Cyber Hygiene tips, check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

DHS CISA Shares Remediation, Risk Guidance for SolarWinds Compromise

The Department of Homeland Security Cybersecurity and Infrastructure and Security Agency (CISA) released an alert warning of a new malware variant, known as SUPERNOVA, which is being used to target vulnerable SolarWinds Orion technology. The report contains indicators of compromise (IOCs) and analyzes several malicious artifacts. Supernova is not part of the SolarWinds supply chain attack described in Alert AA20-352A. CISA has also released new guidance to help support security leaders and administrators with risk decisions and remediation of successful compromises of SolarWinds Orion platforms. The two new resources provide actionable guidance for both private and public industries:

- The Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise web page to provide actionable guidance to organizations affected by this Advanced Persistent Threat (APT) activity. Although the guidance on the web page is directed to federal departments and agencies, CISA encourages affected critical infrastructure and private sector organizations to review and apply it, as appropriate.
- The CISA Insights: SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders supports executive leaders of affected organizations in understanding the threat, risk, and associated actions they should take in response to the APT activity. The CISA Insights specifically applies to organizations with affected versions of SolarWinds Orion who have evidence of follow-on threat actor activity.

CISA encourages affected organizations to review and apply the necessary guidance in the Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise web page and CISA Insights. For general information on CISA's response to SolarWinds Orion compromise activity, refer to www.cisa.gov/supply-chain-compromise.

https://us-cert.cisa.gov/ncas/current-activity/2021/03/09/guidance-remediating-networks-affected-solarwinds-and-active

Resources

CISA

- CISA Ransomware Guide
- CISA Insights on Ransomware Outbreak
- CISA Ransomware Campaign Toolkit

HC3

- Evasive Methods Against Healthcare Threat Brief

Upcoming Events

- April Spotlight Webinar
- 405(d) Spring Campaign! Keep a look out for the 405(d) Program's newest resources called "Myth vs. Fact" and "That Seems Risky."

A Word from 405(d) on PL116-321

The 405(d) Program is encouraged by the passing of H.R. 7898 (public law 116-321) which calls out "approaches promulgated under Section 405(d) of the Cybersecurity Act of 2015" as 'recognized security practices'. We would like to acknowledge the public-private partnership of the 405(d) Task Group for their hard work, dedication, and willingness to collaborate with the U.S. Department of Health and Human Services (HHS) to develop cybersecurity resources, products, and tools.

The 405(d) Program is focused on providing the Healthcare and Public Health (HPH) Sector with useful and impactful resources, products, and tools that help raise awareness and provide vetted cybersecurity practices, which drive behavioral change and move towards consistency in mitigating the most relevant cybersecurity threats to the sector. The public-private partnership is vital to the 405(d) Program as we work towards achieving our mission and ultimately aligning healthcare security approaches across the entire HPH sector.

The passing of this bill not only highlights the work of the 405(d) Task Group and all of its efforts, but it is also another step forward in encouraging HPH entities to continue to focus on cybersecurity practices that will help protect their organizations and their patients. Cyber Safety is Patient Safety. We continue to work with our HHS partners to identify impacts and approaches to ensure all of HHS is working together in response to this new legislation. We hope that the 405(d) Task Group members are encouraged to continue to develop new resources and lend their voices to help define HPH sector cybersecurity best practices moving forward.

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