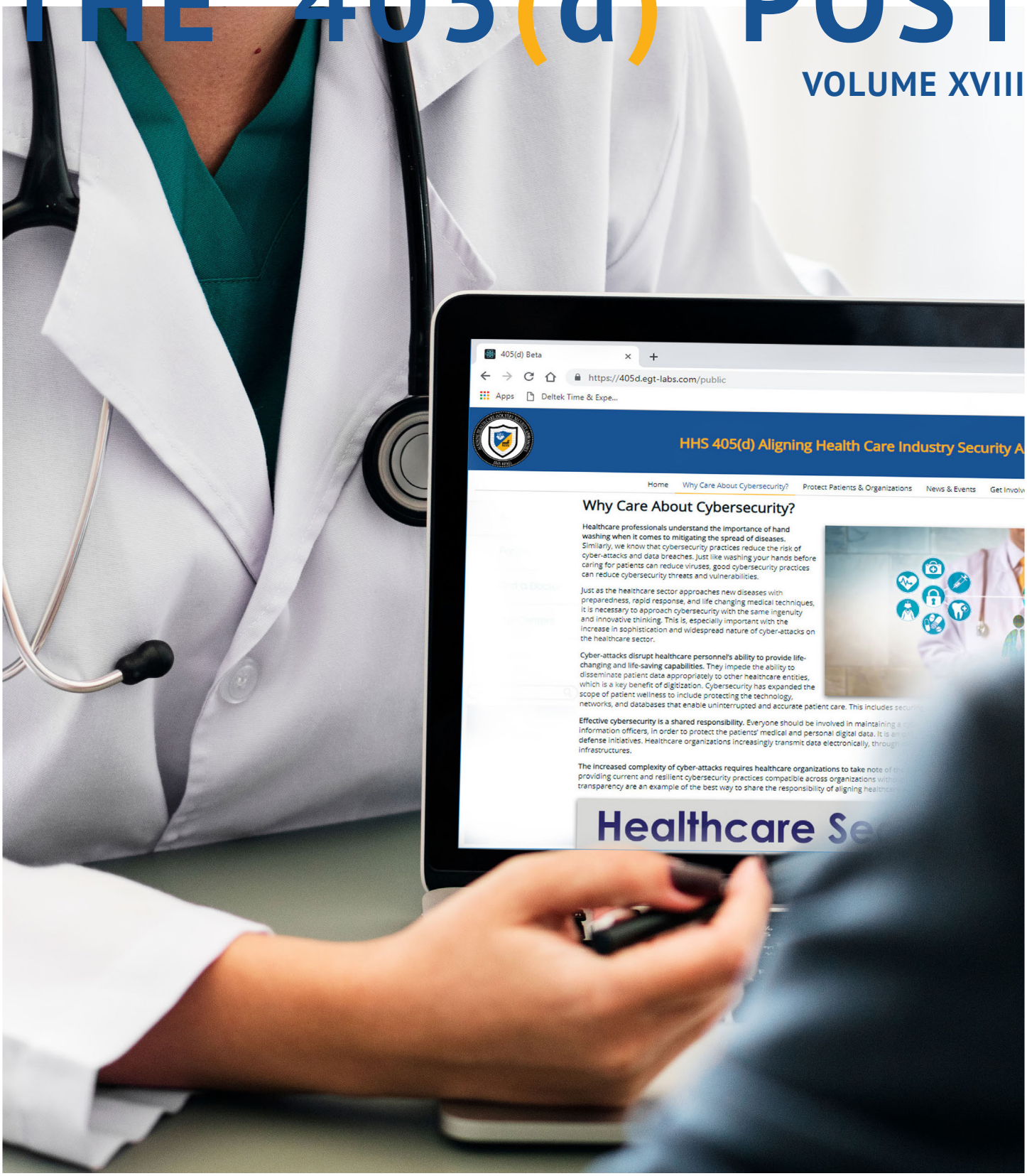
THE 405(d) POST

VOLUME XVIII



HHS 405(d)
Aligning Health Care Industry Security Approaches

A Word from the Task Group

Applying MC² as a Security Professional

By Emily Holmquist, HSCC Model Contract Task Group Member

Clarifying Accountability, Sharing Responsibility for Medical Device Cybersecurity

One of the more thorny cybersecurity issues in the complex healthcare environment involves the security of medical devices in the clinical environment. We know that medical devices have historically not been designed with cybersecurity in mind, and even if they are, widely varying security architecture environments in health delivery organizations make it difficult to ensure robust security against the many evolving and sophisticated cyber threats against healthcare delivery. Many of these ambiguities could be better resolved up front, through the contracting process in which both the buyer and seller have a clear, mutual understanding of respective responsibilities for the security—and safety—of medical devices. Unfortunately, the contracting process across the healthcare ecosystem is uneven, depending on the sophistication and resources of the respective parties.

To address this tension, the Health Sector Coordinating Council (HSCC), has developed a toolkit that offers uniform terminology and fair division of responsibilities between Healthcare Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) in the provision of cybersecurity for medical devices. It is called the Model Contract-Language for Medtech Cybersecurity – or "MC²". As a contributing member of the HSCC task group that produced this essential resource, I was more excited than the average cybersecurity engineer upon its release earlier this year for the industry to quickly adopt the guidance and incorporate the language into every future MedTech contract. Surely, it is evident to my colleagues and business partners how important this material is for streamlining and standardizing medical device agreements.

What is the MC²?

The Model Contract-Language for Medtech Cybersecurity is a reference document that suggests cybersecurity terms and conditions of medical device procurements and servicing between HDOs and MDMs. The framework of MC² includes 14 core principles aligned with industry standards & best practices to address the security safeguards of a medical device in a healthcare environment. This framework represents a joint effort between MDMs, HDOs, and Group Purchasing Organizations to collaboratively ensure patient safety.

As a cybersecurity engineer, I understand the technological aspects of a medical device, but I'm less savvy with the contractual terms and legal jargon. Having an accessible and concise document in my hands to prepare for what often are legal discussions allows me to have an understanding for each term and condition discussed. The same is true for the contract analysts that may not have as strong of an understanding of the technical aspects of the agreement.

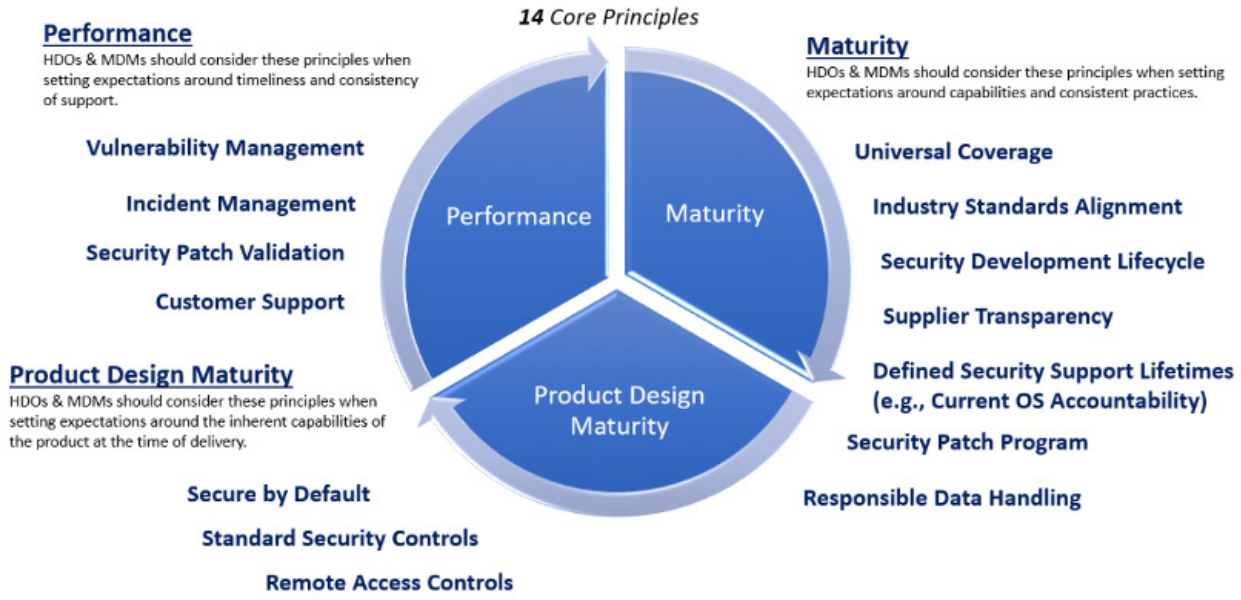


Figure 1. *Core Principles from MC², page 8.*

Is MC² mandatory?

When I discussed the MC² within my previous organization of employment (a medical device manufacturer), my colleagues expressed interest and excitement. There was also some confusion that came from the Contracting team within the organization. As an engineer in the Product Security team, I met with the Contracting team and provided an overview of the MC² to the lawyers, contract analysts, and technical writers. The most popular question from this discussion was, "is this template required by the FDA?" To answer simply, no, the MC² is not an "FDA requirement". **It is entirely voluntary, developed by industry, for industry, and can be tailored to fit the needs of the contract parties during negotiations.** It is intended to assist the relationship between the HDO and the MDM and for their shared responsibility for patient safety and efficacy. The patient is the ultimate benefactor of this guidance, ensuring the HDO and MDM are both following measures to ensure the safety of the medical device in the entirety of its lifespan.

MC² is entirely voluntary, developed by industry, for industry, and can be tailored to fit the needs of the contract parties during negotiations. It is intended to assist the relationship between the HDO and the MDM and for their shared responsibility for patient safety and efficacy.

Who developed MC²?

MC² was developed exclusively by health industry practitioners including providers, medical device manufacturers, and group purchasing organizations. The task group that developed the resource is part of a larger public-private partnership known as the Health Sector Coordinating Council Cybersecurity Working Group, an industry group advising the government and the sector on important elements of critical healthcare infrastructure protection. The HSCC has produced other medical device security resources, such as the Medical Device Joint Security Plan (JSP)—a guide for the secure design, development, manufacture and support of medical devices—and the Medtech Vulnerability Communications Toolkit (MVCT)—a guide for communicating medical device vulnerabilities with appropriate terminology for the intended audience. And, as of this writing in October 2022, a fourth guidance document on the shared responsibility of managing the cybersecurity of legacy medical devices in the clinical environment will be published later in 2022.

How can MDMs/HDOs incorporate the MC²?

At Defcon earlier this year, I discussed medical devices contracts with many HDO security professionals to investigate the HDO angle. One professional I met, head of security for an HDO, wishes to advance security within his organization. However, regarding the MC², the professional shared that "the measures are all well and

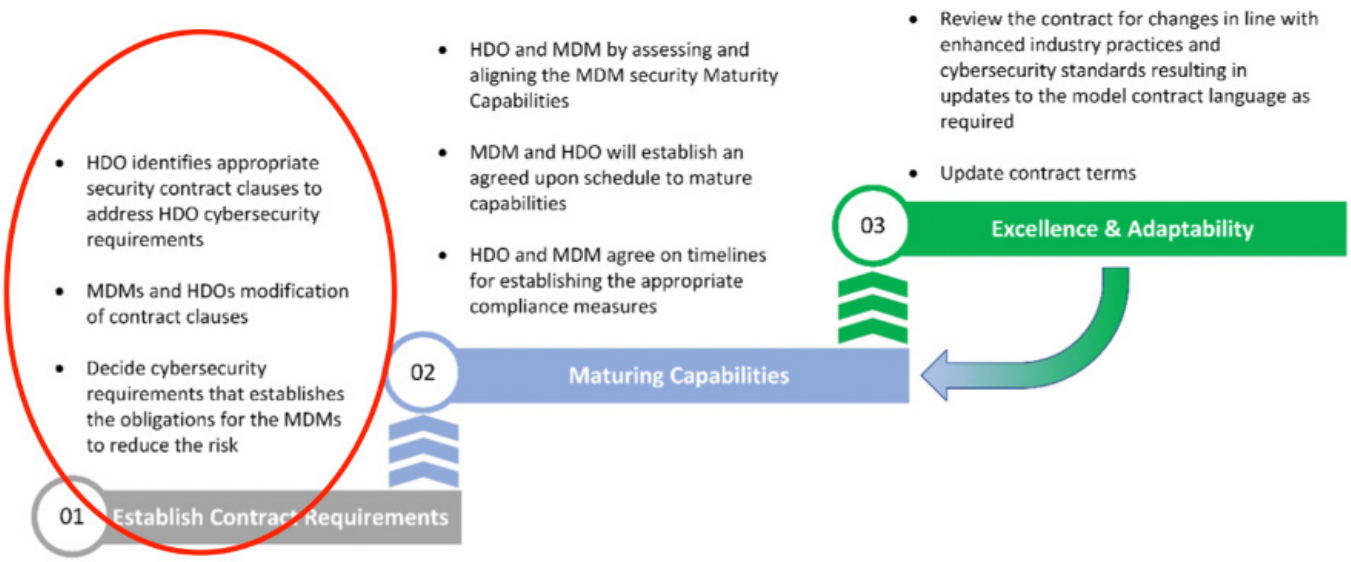


Figure 2. *Partnership Maturity Roadmap from MC², page 7.*

good, but from my own experience I can tell you that they are probably rarely implemented in reality with the necessary consistency." How discouraged I was to hear this! To the extent I'm capable, I'm determined to ensure the adoption of MC². One effort of mine is defining product security requirements closely with the language in MC², where possible. This takes place early in the MDM product development process and ensures the technical controls are implemented and validated, long before a contract is even a consideration. The professional recommends adding network segmentation; "this would get the problem of lateral movement under control," and "this is something that fits quite well into the Attack Surface Reduction & Hardening item," which are clauses 4, 7, 11, and 29 of the MC². This is an important focal point of the MC² for HDOs to consider during the contracting process.

Beyond the product development process and the addition of network segmentation, the MC² may be incorporated in contracting workflows within an MDM. The product security team may drive the awareness of the guidance, and the legal/contracting team may include the guidance formally into the workflow. For example, there are three primary starting points for a contract, 1) the MDM prepares a baseline, 2) the HDO prepares a baseline, or 3) there is no baseline to begin, and both MDM and HDO begin from scratch. Beginning from scratch is the easiest starting point for incorporating the MC². For either the MDM and HDO beginning the baseline, the MC² could be used to draft the internal organization's baseline contract, by selecting all the applicable terms and conditions—refer to Figure 2 above, Step 1: Establish Contract Requirements.

Throughout the negotiation process, the HDO and MDM may always return to the MC² as the neutral participant and referral for contentious terms.

In my experience, there are Work Instructions defined by MDM processes; the contracting team may include the MC² as the reference baseline document in their work instruction for creating an initial agreement with an HDO.

Keep the MC² Momentum Going

Regardless of how the MC² is incorporated, all parties can agree that it is necessary to align and define these contractual terms and conditions for the safety of all patients. Whatever your role within your organization, try to make things better! Whether you are an individual contributor for an MDM, like me, or a leader for an HDO, like Sebastian, the MC² is a starting point for you to begin conversations, with your peers and leaders, to encourage

security progressions anywhere and everywhere possible within your organization. As you read through MC², know that we encourage readers who have adopted some or all the following clauses in your contracts to share observations or recommendations that support a shared understanding about mutual commitments related to the cybersecurity of medical device design and management. Please send your comments at any time to: ContractsFeedback@HealthSectorCouncil.org

About the Health Sector Coordinating Council and the 405(d) Task Group

The HSCC is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is a standing working group of the HSCC, composed of more than 340 industry organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector. The 405(d) Task Group is also a task group that is housed under the HSCC umbrella and provides the sector with industry tested best practices to combat the top 5 cybersecurity threats facing the sector. For more information on the HSCC, see https://healthsectorcouncil.org/. For more information on the 405(d) Task Group see 405d.hhs.gov.

HICP in the Spotlight

OCR Recognized Practices Set Forth in HITECH Amendment

The Office for Civil Rights (OCR) has produced a pre-recorded video presentation that highlights recognized security practices in the 2021 HITECH Amendment signed into law on January 5th, 2021, intended for HIPAA regulated entities. The HITECH Amendment includes standards and approaches outlined in Section 405(d) of Cybersecurity Act of 2015 and Health Industry Cybersecurity Practices: Managing Threats and Patients (HICP) as a recognized approach for HIPAA regulated entities to use.

The purpose of the HITECH Amendment is to incentivize the regulated industry to improve their cybersecurity by implementing recognized security practice (RSP). Implementing a RSP is an entirely voluntary process. OCR will only consider the implementation of a RSP as a mitigating factor in Security Rule investigations and audits.

OCR expects recognized security practices to be implemented throughout the enterprise, OCR expects recognized security practices to be implemented throughout the enterprise, however it is acknowledged that certain elements of RSPs may not be implemented across an entire enterprise or not implemented at all if such practices did not apply to the entire enterprise.

Find out more on The HITECH Amendment along with HICP recognition in the amendment by watching OCR's video presentation on Recognized Security Practices.

Cybersecurity is a Patient Safety Issue

By Mark Jarrett, 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.

How has the cybersecurity environment changed in healthcare? If one thinks back to 15 years ago, our main concern was the theft of personal identifiable information (PII) and protected health information (PHI). People did not want their PII, such as credit card information, nor their healthcare records, stolen. Although these remain serious concerns, a new wave of cyber "insecurity" issues has evolved that threaten the safety of our patients. This risk has increased exponentially as healthcare is now a digitally based industry. To best understand the impact, let us review some examples.

Everyone is now aware of ransomware. Unfortunately, many in healthcare look at this as simply a data hostage situation that requires a payment to resolve. The effect of ransomware, however, on the delivery of care directly affects patient safety. As ransomed medical records are now not available, continuity of care becomes difficult and may not be safe. The medical record is not just to meet administrative and regulatory requirements, it is what clinicians use daily to make medical decisions on care. On a broader level, ransomware disrupts care at the community level. A ransomware attack on a large hospital last year forced them to reduce services. This was not a two-day event but continued for weeks. The attack required shifting offsite of patients, overloading surrounding hospitals, compounded by the added stress of COVID, resulting in delayed care.

Another threat is the cyber vulnerability of medical devices. The healthcare environment is replete with many connected medical devices from IV pumps to implantable devices such as defibrillators. It has been demonstrated that these devices can be hacked. Many devices are unfortunately legacy devices with unsupported software that is insecure. Even newer devices are vulnerable if software upgrades have not been performed. Imagine that the IV pumps are reprogrammed to infuse fatal doses of medications. What if an implanted defibrillator is hacked and now continuously fires a charge. Remember the show Homeland where the Vice President was assassinated by a hacker turning off his pacemaker? Dick Cheney had his pacemaker wireless connection disabled after this show. This is no longer a subject for fiction. There are bad actors, including nation states and terrorists, that could target individuals as well as a whole hospital.

A "white hat" group from Israel was able to demonstrate that they could access the pathway for CAT scan images

traveling from the machine to the PACS system. They manipulated the images to either add or remove masses on lung CAT scans. The radiologist reading the films in almost all cases could not tell that they were altered. The clinical ramifications are frightening.

A new possible scenario is based on healthcare's increasing utilization of artificial intelligence and machine learning (AI/ML). As providers become more dependent on this technology, new vulnerabilities have been recognized. Imagine someone altering the algorithm used for choosing the appropriate chemotherapy for a patient. A provider may decide to follow a false AI/ML recommendation rather than their own choice.

The above risks are not theoretical. Just as ransomware has spread across the healthcare industry, we can all expect that we need to be prepared for the cybersecurity risks outlined above in these limited examples.

What can we do to protect our patients? As always—just being aware is the first step. If a provider is faced with a situation which doesn't make sense, the provider must now think about the possibility of a cybersecurity breach as the etiology. An infusion pump that is not working properly may not be simply due to mechanical failure. If we keep the concept of cybersecurity breaches as a potential cause as we form a differential diagnosis, we are less likely to make an error. The second one is a classic—but still helpful—use strong passwords and multifactor authorization (MFA) whenever possible. Third, be aware of phishing. We all get too many emails each day. It is too easy to open an attachment without thinking. This is often the chink in the armor that allows the hackers in. There are already over a billion devices used to gather health information—from Fitbits to hospital at home monitoring. This area will certainly grow over the next five years but introduces the risks of unsecure home WIFI systems. Patient care has improved with the digital revolution of the last 25 years—but with every opportunity also comes a threat. As healthcare providers, it is our obligation to practice good cyber hygiene to ensure that our patients receive the safest care. One way to start your cybersecurity journey is with the HHS 405(d) Program. The 405(d) program offers a wide variety of cybersecurity resources from technical documents such as the *Health Industry Cybersecurity Practices Publication* (HICP) and resources for cyber hygiene awareness. This program is a constantly providing the sector with up-to-date information for cybersecurity and all of the resources are free! For more information check out their website at 405d.hhs.gov.

Happening Around Us

HSCC Focuses on Medical Device Security in New Contract Language Template

The Healthcare & Public Health Sector Coordinating Counsels (HSCC) released a contract language template for healthcare organizations to utilize when working with medical device manufacturers (MDMs). The template provides contract language and security requirements for MDM's around storing, securing, and transferring data on network connected medical devices. The template can be utilized by any size organization but should to be tailored to fit your organizations device security needs.

Read the full article here.

Medical Device Security Requires Standards, Shared Responsibility

The need for supply chain security standards is an increasingly important topic due to medical device security challenges in healthcare organizations today. In an article titled "Medical Device Security Requires Standards, Shared Responsibility" researchers discuss the collaboration needed between manufacturers and providers when working through the medical device acquisitions process.

Read the full article here.

Hospitals Continue to Suffer Impacts of CommonSpirit IT Security Incident

In an article published on October 12, 2022, we visit the effect of an IT security incident that has limited the functionality of hospitals across the country. Due to the attack, hospitals are being forced to take their EHR systems offline. The target of the attack is one of the largest healthcare systems in the United States.

For more on this story, read the full article here.

Other Resources

HC3

Abuse of Legitimate Security Tools and Health Sector Cybersecurity

OCR

OCR Settles Case Concerning Improper Disposal of Protected Health Information

FDA

FDA Cybersecurity Page

CISA

Cybersecurity Awareness Month 2022: See Yourself in Cyber

Cybersecurity Awareness Month 2022: See Yourself in Cyber — Public Toolkit

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. The news articles are not an endorsement of any product/viewpoint/entity. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations.

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

Follow us!

Facebook Twitter

Instagram LinkedIn

Visit our website at 405d.hhs.gov!