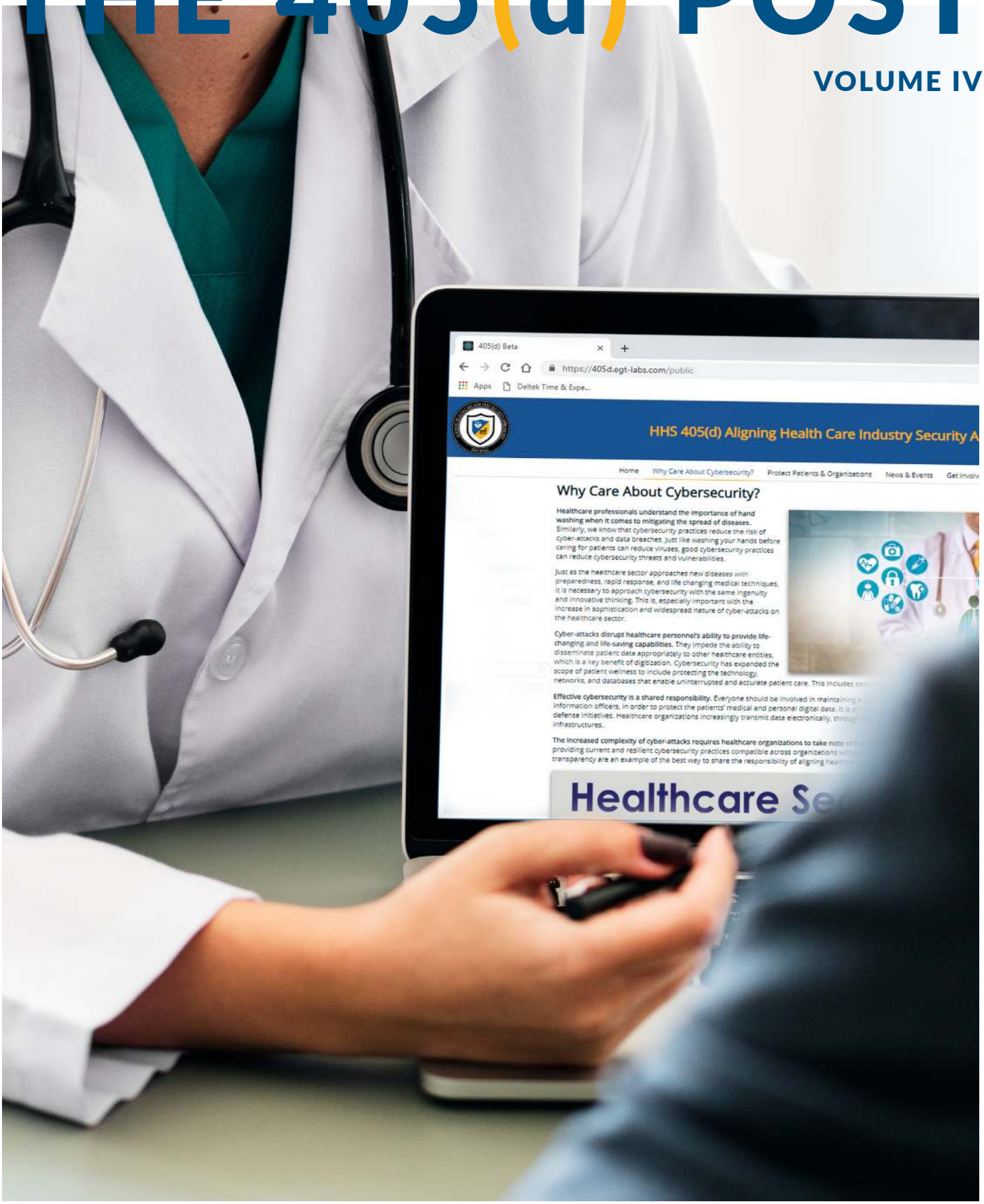
THE 405(d) POST

VOLUME IV



HHS 405(d)
Aligning Health Care
Industry Security Approaches

How MDS² Data Can Inform Smarter Medical Device Workflows

By Ido Geffen and Priyanka Upendra, 405(d) Task Group Members

In 2004, NEMA (the National Electrical Manufacturers Association) together with HIMSS (the Health Information Management Systems Society) and a number of other security experts and government agencies produced a short document template for manufacturers to use in order to describe the vital security properties of their devices. They named this document the "Manufacturer Disclosure Statement for Medical Device Security" — which is generally shortened to MDS² .

What Is In the MDS² Form?

The MDS² form is the medical device manufacturer's response to its clinical users on the security and privacy controls of the devices. Without this visibility, they can't set up effective risk management strategies. The MDS² differs from a software or hardware Bill of Materials in the sense that it conveys product information in a much more descriptive and selective manner. So whereas a software bill of materials would simply list all the software components included in the device, an MDS² form for the same device would describe the product in terms of its cybersecurity capabilities and/or compatibilities and the immediate implications thereof.

In a way, you can think of it like this: the bill of materials is like the list of ingredients on the back of your food package, while the MDS² is more like the nutritional facts; only instead of nutrition, it's about cybersecurity. Because the MDS² forms aim to establish a standard template, if thoroughly consumed, they stand to provide a way to develop better security strategies for medical devices deployed in clinical settings.

The MDS² captures and contextualizes medical device security information through a list of short questions covering a range of different categories. By design, most of the questions prompt simple and direct yes-or-no answers so that there's little room for interpretation and confusion.

Over the years, there have been several new versions of the MDS² developed and — as with any

good model — it is constantly being reexamined and assessed with an eye toward improvement. The most recent and most significant changes to MDS² were released in 2019. This latest version goes both deeper and wider in capturing medical device security attributes — more than double the questions addressing security control questions, adding new sections on remote service, administration capabilities, connectivity capabilities, software roadmaps, the management of personally identifiable information, and the software bill of materials (SBOM). Practically speaking, the information and context provided in MDS² forms can help to:

- Point you to the top security concerns and considerations to keep an eye on
- Index the device's primary security characteristics
- Capture interoperability and cybersecurity requirements/implications
- Reflect the vendor's long-term support and liability commitments.

For hospitals, smart utilization of MDS² forms can also help streamline workflows and add value across a number of different departments. Consider the following examples:

- For IT teams, MDS² can — help optimize device deployments, provide information on standard port configurations, network connectivity parameters, and supported communication types;

- For IS teams, MDS² can — help build device risk profiles, inform on effective risk mitigation and management strategies, define anti-virus requirements, and gauge the likely system and data impact of a given device's compromise;

- For Compliance teams, MDS² can — provide insight on the type of data a device is designed to handle and the type of privacy controls or compatibilities the device is subject to (does a device locally store protected health information? Is there encryption? Is encryption applied only to data at rest or in transmission as well? Etc.);

- For HTM teams, MDS² can — guide management efforts aimed at operational resilience, assist maintenance and lifecycle management, and help to more intelligently plan for long-term support.

Encouraged Adoption

To see more universal MDS² utilization, we encourage regulators to step in with a first guiding hand. Ideally, MDS² documentation would accompany all medical device sales. In the meantime, we just need to push for increased cyber consciousness and advocate for greater MDS² adoption. In recent years, the needle has indeed begun moving in that direction. Many hospitals now insist on up-to-date MDS² documentation as part of the procurement process. For the industry as a whole, this is very encouraging.

Hopefully, we'll soon reach a time when buyer committees consider MDS² forms an integral part of their purchase decision. When that happens, manufacturers who offer stronger security controls and more advanced authentication, access protection, and auditing capabilities will be trusted providers of medical devices — empowering an industry-wide hardening of security.

Moving Forward

To draw MDS² out of the filing cabinet and put it into regular use, you need to first build it into your strategic planning, then into your processes and operational technologies. By planning ahead

and integrating MDS² forms into your standard workflows, HTM, IT, compliance, and IS teams can be more precise and surgical with each motion — removing guess work and ultimately building smarter, safer, and faster processes.

Leaders from all these teams should meet to discuss how to make the best use of MDS² forms. They should plan how to use the data, as well as when to use MDS² information as a shared frame of reference for all stakeholders to gather around. Since the consensus of the hive mind alone will not get people used to working with MDS² in the course of their daily tasks, it's also important to build a MDS² best practices curriculum and hold some training sessions. Write out and formalize your standard operating procedures and highlight where MDS² plays in.

Once you have a well thought out and well-defined plan in place for how to regularly leverage your MDS² forms, you'll need to build it into your operational infrastructure. That means integrating MDS² into your workflows and toolbox in such a way that your above-defined SOP can flow naturally and fluidly without encountering silo or out-of-process issues.

You'll want to make sure that your MDS² forms are fully digitized and integrated into your CMMS and HIT management databases so their contents can be easily indexed and searched. Pulling on this data integration, you may want to configure automated notifications or alerts based on your fleet, its MDS² characteristics, device lifecycle milestones, and cross-referenced vendor advisories.

As much as possible, it's important to avoid manual work and the introduction of redundant or overlapping tooling. The best way to make sure that the information is actually seen and used is to build it into the tools that your teams are already using.

Once you have a manageable system in place that allows you to search and retrieve specific pieces of security information based on the device or risk dimension of your choosing, you can conduct quantitative and qualitative risk analyses. The goal should be to identify any cybersecurity control gaps, bridge those gaps, and then work to design effective risk mitigation and management regimes.
The best practice would be to establish a five-step process:

1. Identify risks
2. Apply common controls
3. Identify control gaps
4. Apply compensatory controls
5. Manage residual and uncontrolled risks

Of course, those are five long and complicated steps; and when you finish working your way through them, you'll likely have more devices to integrate into the process and an evolved threat landscape to factor into your risk profiling. Cybersecurity is neither quick nor simple, but it is vital if hospitals are to continue delivering care safely, securely, and reliably in modern world. To that point, better use of MDS² information can be a key enabler for healthcare excellence — across IT, IS, HTM, and compliance teams. Through smart system and process based integration, MDS² can and must be better leveraged by hospitals and medical centers.

Healthcare technology management (HTM) is the name of the field responsible for managing the selection, maintenance, and safe and effective use of medical equipment and systems. This field includes biomedical equipment technicians (BMETs), clinical engineers, imaging equipment specialists, laboratory equipment specialists, and others who protect patient safety and reduce healthcare costs related to technology.

HICP Spotlight

Cyber Safety Is Patient Safety

March 8-14, 2020 was Patient Safety Awareness Week and the 405(d) message was and always has been: Cyber Safety is Patient Safety. The Patient Safety Awareness Week campaign was an annual recognition event to encourage the public to learn more about healthcare safety and we believe this should and does include cybersecurity. Cyber-attacks in healthcare affect every aspect of an organization but most importantly they affect patient safety. A single cyber-attack has the potential to shut down care facilities, erase important patient health history, and put your patient's health and identity at risk. The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) Publication provides organizations details about the top five threats facing the healthcare industry and ten practices that can be implemented to mitigate them. Ensuring the American public is safe in their healthcare system is a priority for HHS and this involves cybersecurity. Read a message from the HHS CISO Janet Vogel as she discusses the importance of cybersecurity as it relates to patient safety.

Letter from HHS Chief Information Security Officer

Dear Colleagues,

Dear Colleagues,
At some time in our lives all of us are or will become patients in the healthcare system. This can be a daunting experience and a vulnerable one because you are immediately placing your trust in healthcare professionals to keep you safe and secure. As part of the annual **Patient Safety Awareness Week** across the United States, we are participating in this campaign to encourage the public to learn more about healthcare safety. We at HHS believe this must, and does, include cybersecurity. Our theme for HHS is "**Cyber Safety is Patient Safety**."

There has never been a more critical time for our sector to discuss the importance of cybersecurity as it relates to patient safety because an increase in cyber-attacks have crippled hospitals, doctor's offices, and other care facilities. HHS wants to do everything we can to help the healthcare community do what it does best - care for and protect patients.

HHS has two programs that are available to the public to prepare for and mitigate cyber-attacks. The first is the HHS 405(d) Program which aims to align healthcare industry

security approaches. This program created the **Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)** publication to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the most pertinent cybersecurity threats. The second is the **HHS Health Sector Cybersecurity Coordination Center (HC3).** In order to address these threats, HC3 works across the health sector, including healthcare organizations, law enforcement, and cybersecurity information sharing organizations, to understand the threats our sector faces, learn the bad actors' patterns and trends, and provide information and approaches on how the sector can better defend itself.

Last week, the 405(d) Program sent out cybersecurity awareness materials that you can use throughout your organizations to increase awareness of this ever growing threat to our industry. I encourage you to use these to educate your workforce and instill the concept that Cyber Safety is Patient Safety. If we as a committed group continue to spread awareness, we will succeed at moving the needle and continue to protect our patients.

Thank you,

Janet Vogel
Chief Information Security Officer
U.S. Department of Health and Human Services

The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) Publication

Happening Around Us

Cybersecurity Experts on Alert after Iran Strike

NBC NEWS

NBC News reports, cybersecurity professionals across the U.S. expressed a mixture of concern and caution after news broke that the United States had killed Gen. Qassem Soleimani, a high-profile Iranian military commander in Iraq. Many are explicitly saying that they are gearing up for potential retaliation from Iran, which has already proven in recent years to be a formidable adversary in the cyber realm. Iran is considered one of Washington's primary adversaries in cyberspace, and has shown a willingness to go after government and civilian targets. While Iran has also engaged in social media disinformation campaigns and hackers have defaced websites, cybersecurity experts have said they're particularly concerned about potential breaches of major U.S. companies and government agencies that work with crucial infrastructure. Cyber operations take time, and if Iran does intend to conduct a retaliatory destructive cyberattack for Soleimani's death, it will need to first gain a foothold in target networks which is something it has in the Middle East more than in the U.S.3 Check out our Resources Section to learn more about this threat from the DHS Cybersecurity and Infrastructure Security Agency (CISA).

Evasive Domain-Impersonation Phishing Attacks Increase by 400%

HEALTH IT SECURITY NEWS

Researchers at a cybersecurity firm detected a 400 percent increase in domain-impersonation attacks designed for conversation hijacking since July. While this method is used far less frequently than other phishing attack methods, the sophisticated and targeted nature makes the threat more effective. The research team analyzed more than 500,000 monthly email attacks from July 2019 to November 2019. In July, they detected just 500 of this type, compared with more than 2,000 attempts in November. To steal sensitive personal information, money, or change payment details, hackers leverage conversation hijacking in which an attacker sends emails within an actual conversation from the victim's email account. The researchers explained that the hackers can also initiate new conversations based on intel they've collected from compromised accounts or other sources.[2] To find out how to protect your organization from email phishing attacks, access The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) Publication

Hackers Demand Ransom Payments From Patients of Florida Provider

BECKERS HOSPITAL REVIEW

The patients of a Florida healthcare provider were victims of a ransomware attack in which the cybercriminals claimed to have access to patient data and that it would be publicly exposed if the provider did not pay the ransom. The provider filed a complaint with FBI Cyber Crimes, and installed new hard drives, firewalls and malware detection software. It is estimated that the personally identifiable information of up to 3,500 former and current patients may have been exposed during the ransomware attack. Patients who have been threatened with ransom demands are urged to report the incident with the FBI.[2] To learn more about Ransomware and the ten best practices to mitigate this threat access The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) Publication

405(d) Events and Announcements!

405(d) Spotlight Webinar:
Securing Medical Devices
Wednesday April 15th at 1pm EST!

405(d) is live Social Media!
The 405(d) Program is taking our mission of aligning healthcare security approaches to Twitter, Facebook, and Instagram! Follow Us, the 405(d) initiative @Ask405d to learn about cybersecurity best practices and the five main cybersecurity threats, plus upcoming events and engagements. Check us out!

Additional Resources

FDA Fact Sheet: The FDA's Role In Medical Device Cybersecurity

HC3 Sodinokibi Ransomware Whitepaper

HHS HC3 Briefing: Ransomware Threat to State and Local Governments

HHS Office For Civil Rights Ransomware Guidance

HHS Office for Civil Rights Cyber Attack Check-List

HHS Office for Civil Rights Cyber Attack Response Infographic

Iranian Cyber Response Alert

Happening Around Us Sources

1. BECKERS HOSPITAL REVIEW
2. HEALTH IT SECURITY NEWS
3. NBC NEWS

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" 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 or visit our website at 405d.hhs.gov!