ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Left to our own *Devices* – Will we follow best practices?

Ty
Industry Principal, Healthcare
Medigate by Claroty
Ty.G@Claroty.com

Skip Sorrels
Director, Cyber Security
Ascension Technologies

Jon Benedict
Medical Device Security Principal
CynergisTek
Jon.Benedict@CynergisTek.com

MEDIGATE by Claroty

Ascension

CYNERGISTEK A Clearwater Company

November 15, 2022

ACCE gratefully acknowledges the sponsorship of this webinar by

About the Moderator

Juuso Leinonen

Principal Project Engineer
ECRI

Juuso Leinonen is a Principal Project Engineer, at the Device Evaluation group at ECRI, where he performs comparative medical device evaluations and investigates medical device related accidents. His current subject-matter expertise includes infusion technology, medical device cybersecurity, and telehealth.

Logistics

- All attendees have their microphones muted during the presentation.
- Questions to the panelists must be submitted via the “Q&A” feature (not chat) in Zoom at any time.
- If there is any urgent issue, please use the “chat” feature to communicate with the panelists.
- We will try to ask Ty, Skip and Jon to answer questions not addressed during the webinar and distribute them to participants via email or post them to ACCE website.
- Please remember to complete the webinar evaluation after attending. A link will be provided at the end.

About the speaker

Ty Greenhalgh, HCISPP
Industry Principal, Healthcare

MEDIGATE
by Claroty

Ty is currently the Healthcare Industry Principal with Medigate by Claroty. Claroty, a worldwide leader in cybersecurity, empowers organizations around the world to secure all their cyber-physical systems. Claroty recently purchased Medigate, the Best in KLAS healthcare solution, integrating the tools required for cybersecurity of medical devices to become the dominant leader for healthcare device cybersecurity.

Ty holds the position of Ambassador with the HHS 405(d) Program and Task Group which was responsible for the recognized security practices referenced in the new HITECH amendment more commonly known as the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.*

He was employed with 3M Health Information Systems for over 25 years. He helped introduce disruptive technologies to include Electronic Health Records, Remote Transcription, Digital Dictation and Speech Recognition, Document Scanning, Computer Assisted Coding and Computer Assisted Clinical Documentation Improvement.

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

About the speaker

Jon Benedict
Medical Device Security Principal
CynergisTek

Mr. Jon Benedict is Medical Device Security Principal at CynergisTek. Mr. Benedict is responsible for the definition, creation, and execution of the customer-facing Medical Device Cybersecurity program. He oversees the assessment and coordination of cybersecurity standards, policies, and procedures for CynergisTek's Healthcare Delivery Organization (HDO) clients.

Before joining CynergisTek, he spent more than 25 years in multiple leadership positions, where he has a proven track record of managing the development and delivery of specialized IT and IT Security solutions for customers in healthcare, telecommunications, and the energy sector, by leveraging his unique blend of expertise working with OEM's, Clinical Engineering and Healthcare Delivery Organizations IT Security departments.

About the speaker

Skip Sorrels
Director of Cybersecurity
Ascension Technologies

Skip Sorrels is Director of Cybersecurity for Ascension Technologies having oversight across Ascension for cyber and information security operations. He is responsible and directs the following programs: standards and policies (GRC), vulnerability management, privileged access management, threat intelligence, pen testing, medical device and operational technologies cyber security.

Previously, Skip served as Dell and then NTT's Program Executive of service delivery for Ascension as well as for AMITA Health. He is a graduate of the University of Arkansas for Medical Sciences.

Session Description

The White House announced their intention to release security directives targeting healthcare IoT devices. The Joint Commission has begun constructing a new audit for the cybersecurity of connected medical devices. Congress passed a HITECH amendment offering financial protection and relief from costs associated with a breach. The Office for Civil Rights is increasing their investigation team by 60%. The HHS 405(d) group is releasing an updated version of the Healthcare Industry Cybersecurity Practices (HICP) in November.

Offering both carrots, sticks, and guidance, government agencies are trying to get the private sectors attention on securing hospital networks. Despite all the discussion, medical devices remain vulnerable to cyberattacks and while financially devastating, it is more importantly a threat to patient safety. Join us in this webinar for a high-level discussion on Medical Device Security best practices:

1. The Department of Health and Human Services suggested best practices.
2. What does the new HITECH law offer for incentives to adopt cybersecurity?
3. What are the Recognized Security Practices (RSP) in the HITECH Law?
4. Why are these RSPs different for medical devices than IT devices?
5. Which RSPs will have the most impact on Clinical Engineering and HTM?

Government Agency Activity

- FDA Guidance - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions [1]
- Protecting And Transforming Cyber Health Act – HR 7084 [2]
- Strengthening Cybersecurity for Medical Devices Act – S 4336 [3]
- White House National Security Advisor - Healthcare Directives (Devices)[4]
- FDA User Fees – Stripped Medical Device Security Initiatives [5]
- New OCR Director Fontes Ranier – doubling investigators [6]
- CISA Cross-Sector Cybersecurity Performance Goals [8]
- White House signaling for Security Directives for Healthcare [7]

White House New Cybersecurity Standards

October 20th, 2022

- Healthcare is one of the main focus areas for the White House, and efforts to improve cybersecurity across the sector are underway. Neuberger confirmed that the Department of Health and Human Services has been working with partners at hospitals and has been developing minimum cybersecurity guidelines and will be working on developing new standards and guidance for securing medical devices and other broader areas of healthcare in the near future.

The Joint Commission's New Audit

The Stick

- HHS OIG Report to CMS – June 2021
  - Medicare Lacks Oversight of Cybersecurity for Connected Medical Devices
  - CMS engaged The Joint Commission
    - Interpretive Guidelines and Conditions of Participation (CoP)

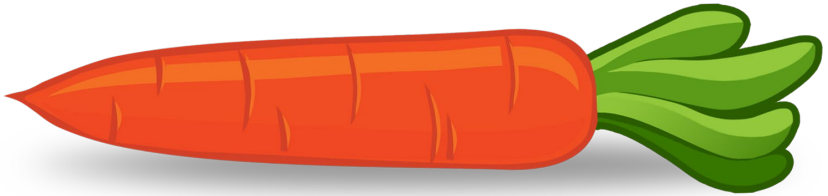
HDOs will invest in XIoT Cybersecurity to avoid financial penalties from failing The Joint Commission audits

https://www.oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000446.asp

HITECH Amendment

H.R.7898 — 116th Congress (2019-2020)

Signed January 5, 2021 | Public Law No: 116-321



Public Law 116–321
116th Congress

An Act

Jan. 5, 2021
[H.R. 7898]

To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. RECOGNITION OF SECURITY PRACTICES.

Part 1 of subtitle D of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.) is amended by adding at the end the following:

42 USC 17941.

"SEC. 13412. RECOGNITION OF SECURITY PRACTICES.

"(a) IN GENERAL.—Consistent with the authority of the Secretary under sections 1176 and 1177 of the Social Security Act, when making determinations relating to fines under such section 1176 (as amended by section 13410) or such section 1177, decreasing the length and extent of an audit under section 13411, or remedies otherwise agreed to by the Secretary, the Secretary shall consider whether the covered entity or business associate has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place that may—

"(1) mitigate fines under section 1176 of the Social Security Act (as amended by section 13410);

"(2) result in the early, favorable termination of an audit under section 13411; and

"(3) mitigate the remedies that would otherwise be agreed to in any agreement with respect to resolving potential violations of the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title) between the covered entity or business associate and the Department of Health and Human Services.

"(b) DEFINITION AND MISCELLANEOUS PROVISIONS.—

"(1) RECOGNIZED SECURITY PRACTICES.—The term 'recognized security practices' means the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the covered entity or business associate, consistent with

Amend HITECH Act - consider **certain *recognized security practices***

HHS must consider it when making decisions for things like audits and enforcement

Demonstrate recognized security practices for at least the previous 12 months

HHS can take **Recognized Security Practices** into consideration to:

1. Reduce fines
2. Decrease length of audits/increased favorable result
3. Mitigate remedies during Settlement negotiations (CAP's, etc.)

Recognized Security Practices

1. NIST
2. **405(d) – Cybersecurity Act of 2015**

https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf
https://journal.ahima.org/page/navigating-the-new-hipaa-safe-harbor

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Recognized Security Practices

Nick Heesters - Sr. Cybersecurity Advisor OCR

HHS 405(d)

Medical Device Security

Aligning Healthcare industry Security Approaches

HHS 405(d) PROGRAM

Aligning Health Care Industry Security Approaches

What is the 405(d) Program?

Cybersecurity Act of 2015 (CSA)

CSA Section 405

Improving Cybersecurity in the Healthcare Industry

Section 405(b)
Healthcare Industry Preparedness Report

Section 405(c)
Healthcare Industry Cybersecurity Task Force

Section 405(d)
Aligning Healthcare Industry Security Approaches

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Section 405(c)
Healthcare Industry Cybersecurity Task Force

405(c)

Health Care Industry Cybersecurity Task Force Report

6 IMPERATIVES

1. NIST CSF for leadership and governance
2. Security and resilience increased
   - *medical devices & Health IT*
3. Improve information sharing
4. Cybersecurity training & awareness
5. Develop workforce
6. Protect R&D and Intellectual Property

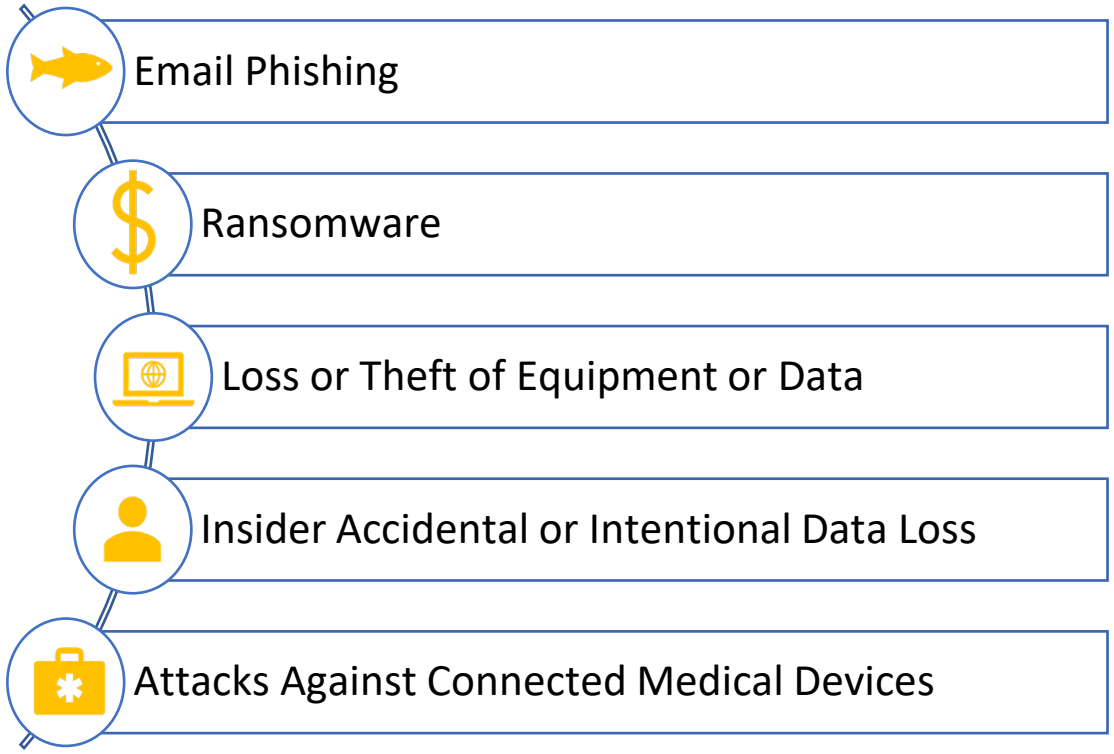
405(d) Task Group

The core of the 405(d) program is it's task group members. Convened by HHS in 2017, the 405(d) task group is comprised of over **230 +** information security officers, medical professionals, privacy experts, and industry leaders.

The task group members help drive all aspects of the 405(d) program, to include official program products, awareness campaigns, engagements, and outreach channels.

The task group is actively collaborating and working on a host of new resources for the sector including an update to the HICP publication and a new ERM Cybersecurity publication both of which are planned to be released in 2021/early 2022

Top 5 Most Impactful Cybersecurity Threats



Top 10 Most Impactful Mitigations

1. **Email Protection Systems**
2. **Endpoint Protection Systems**
3. **Access Management**
4. **Data Protection and Loss Prevention**
5. **Asset management**
6. **Network Management**
7. **Vulnerability Management**
8. **Incident Response**
9. **Medical Device Security**
10. **Cybersecurity Policies**

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

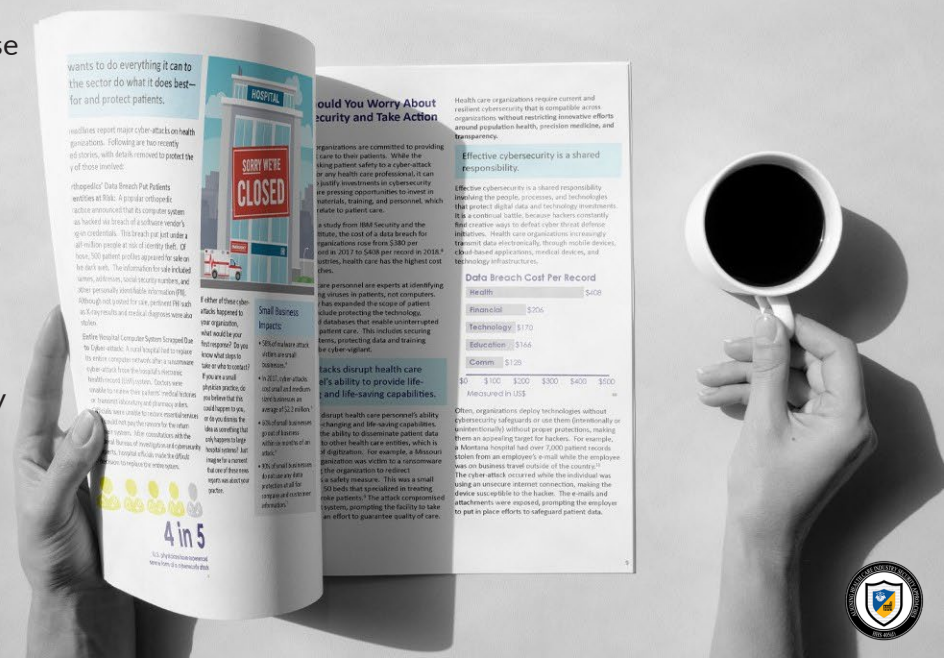
405(d)'s Cornerstone Publication

After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a main document and two technical volumes, and a robust appendix of resources and templates.

The **Main Document** examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.

Technical Volume 1 discusses these ten cybersecurity practices for small healthcare organizations.

Technical Volume 2 discusses these ten cybersecurity practices for medium and large healthcare organizations.



HICP – 2022 Release

Cybersecurity Practice #9: Medical Device Security

Healthcare systems use many diagnostic and therapeutic methods for patient treatment. These range from technological systems that capture, render, and provide detailed images of scans to devices that connect directly to the patient for diagnostic or therapeutic purposes. Medical devices range from straightforward monitors,

Medical Device Management

Medical devices that can connect to the internet are a specialized type of IoT device, specific to providing clinical diagnosis or treatment within HDOs. Nevertheless, cybersecurity for medical devices requires many of the cybersecurity practices already discussed in this document:

- Cybersecurity Practice #2: Endpoint Protection Systems
- Cybersecurity Practice #3: Identity and Access Management
- Cybersecurity Practice #5: IT Asset Management
- Cybersecurity Practice #6: Network Management
- Cybersecurity Practice #7: Vulnerability Management
- Cybersecurity Practice #8: Security Operations Center and Incident Response

Rather than recreating these cybersecurity practices, HDOs are encouraged to extend the relevant cybersecurity practice from each section, implementing it appropriately for medical device management. The following sections expand on how the practices listed above apply in the specialized case of medical devices.

Areas of Impact

PHI

Medium Sub-Practices

- **9.M.A** Medical Device Management
- **9.M.B** Endpoint Protections
- **9.M.C** Identity and Access Management
- **9.M.D** Asset Management
- **9.M.E** Vulnerability Management
- **9.M.F** Contacting the FDA

Large Sub-Practices

- **9.L.B** Security Operations and Incident Response
- **9.L.C** Procurement and Security Evaluations

Key Threats Addressed

- Attacks against medical devices that can affect patient safety

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Asset Management

- Inventory: Software & Hardware
- Automated Asset Discovery
- CMMS

New Term (ADS):

Automated Discovery & Security solution

Practice 9:M:A

Endpoint Protection Systems

- Agents
- Integration
  - Patch Levels of OS
  - EDR possible?
- Unused Ports

Practice 9:M:B

Identity & Access Management

- Authentication
- MAC Authentication Bypass
- Default Passwords

Practice 9:M:C

Network Management

- Network Segmentation
- Zero Trust Architecture
- Automated Policy Generation

Practice 9:M:D

Vulnerability Management

- Risk Categorization
- Vulnerability Disclosure
- SBoM
- Vulnerability Scanning

Practice 9:M:E

Procurement & Security Evaluations

- Security Evaluations
- Risk Scoring
- Contract Negotiation
- SBoM
- EOL/EOS

Practice 9:L:B

Closing Comments

Medigate aligns with the 405(d) HICP

Medigate's Deep Packet Inspection (DPI) provides required granular VISIBILITY

HITECH Law offers protection – fines, fees, post breach oversight

The Joint Commission's new audit is coming

The White House is signaling for new directives

Where is your organization on the journey?

Resources

1 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

2 https://www.congress.gov/bill/117th-congress/house-bill/7084/text?r=1&s=1

3 https://www.congress.gov/bill/117th-congress/senate-bill/4336?q=%7B%22search%22%3A%5B%22S+4336%22%2C%22S%22%2C%224336%22%5D%7D&s=1&r=1

4 https://www.axios.com/2022/10/14/white-house-cyber-regulations

5 https://healthitsecurity.com/features/experts-weigh-in-on-medical-device-security-exit-from-fda-user-fee-bill

6 https://thedailycable.co/08/28/politics/578878/hackers-have-laid-siege-to-u-s-health-care-and-a-tiny-hhs-office-is-buckling-under-the-pressure/

7. https://www.meritalk.com/articles/white-house-eyeing-cyber-work-on-comms-water-healthcare-sectors/

8. https://www.cisa.gov/cpg

Thank You

Please complete the online evaluation/attendance form at https://www.surveymonkey.com/r/11-15-22_ACCE-Medigate

Jon Benedict – Jon.Benedict@CynergisTek.com

Ty Greenhalgh – Ty.G@Claroty.com