CONFIDENTIALITY
COALITION

GENERAL COMMITTEE MEETING

Thursday, February 22, 2018
3:00 PM to 4:00 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

Conference Line: 857-232-0157, 30-40-73#

1. **Welcome and introductions**

2. **Guest Speaker: Greg Garcia, Executive Director for Cybersecurity of the Healthcare Sector Coordinating Council (HSCC)** **Attachment 1,2,3**

3. **Discuss TEFCA comment letter** **Attachment 4**

4. **42 CFR Part 2 letter** **Attachment 5,6**

Next Meeting Date: 3/12, noon - HIPAA 101 Briefing

Attachment 1

Greg Garcia

Greg Garcia served as the nation's first Assistant Secretary for Cyber Security and Communications at the U.S. Department of Homeland Security from 2006-2008, where he led the National Cyber Security Division, the National Communications System and the Office of Emergency Communications. Under Greg's leadership, DHS was a key driver in the development of President Bush's Comprehensive National Cyber Security Initiative (HSPD 23), the National Emergency Communications Plan, and the precursor to what is now the National Cyber and Communications Integration Center (NCCIC). Greg was later brought on to develop and manage an external strategy for cyber security and identity management partnerships for Bank of America until December 2011. Greg was also Executive Director for the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). Prior to FSSCC, Greg was President of Garcia Cyber Partners, a business development and strategic partnerships advisory firm for cyber security, government business, financial services and information technology, and served as an advisor to the Financial Services Information Sharing and Analysis Center (FS-ISAC). Garcia has led initiatives from a variety of technology and public policy positions, including Vice President, Information Security Policy and Programs with the Information Technology Association of America; professional staff member for the U.S. House of Representatives Committee on Science; Director of Global Government Relations Director at 3Com Corporation; and International Trade Vice President at the American Electronics Association. He is the principal staff author of the Cyber Security R&D Act of 2002 and has achieved many government policy changes throughout his career for the benefit of security and economic growth. He is a member of the Information Security and Privacy Advisory Board, a federal advisory committee, and has occupied various advisory board positions with high tech startups.

Attachment 2

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Date: January 9, 2018

To: Healthcare Association Stakeholders (*recipients at bottom*)

From: Healthcare Sector Coordinating Council Cybersecurity Working Group (CWG) Co-Chairs:
Terry Rice, Merck
Bryan Cline, HITRUST

Cc: Greg Garcia, HSCC CWG Executive Director

Subject: **February 6 Healthcare Sector Coordinating Council Cyber Working Group DC Meeting**

This is a call to action to the healthcare sector to coalesce around the urgency of protecting our information and operational infrastructures against cyber threats.

Each of your associations represents a critical subsector of the healthcare industry, and each is part of an interdependent ecosystem that is facing increasingly sophisticated cybersecurity threats and vulnerabilities that can cascade across the value chain of the healthcare sector, ultimately affecting patient safety, security and privacy. We know you will agree it is our collective responsibility to deliver industry-wide policy and operational solutions to this shared challenge.

Our responsibility. This responsibility is captured in three iterations of a Presidential Executive Order dating to 1998, the most recent being Presidential Policy Directive 21 in 2013, which calls on 16 critical industry sectors to self-organize – in partnership with the government - around the mission to protect essential assets and services from existential threats. Every critical industry sector, including healthcare, financial services, electricity, emergency services, communications, water, transportation, and others, has been stepping up to this mission. We do this with two essential functions: the day-to-day operational protection, threat analysis and incident response of the National Health Information Sharing and Analysis Center (NH-ISAC), and the longer-term strategic and policy-oriented mission of the Healthcare Sector Coordinating Council (HSCC).

What is the HSCC and what does it do? We have had discussions with many of you about the HSCC – recognized under the Executive Order as the private industry partner to the Department of Health and Human Services. The HSCC is in effect an association of associations, which also must include your members, convening at the HSCC "big table" to identify and attack those cross cutting threats and vulnerabilities that challenge our ability to deliver safe and secure healthcare to the nation. We do this both independent of, and in partnership with, the Department of Health and Human Services – our "sector specific agency." During designated working sessions between government and industry, competitive and regulatory equities are left outside the door, and sensitive information discussed with the government is *afforded protection from public disclosure under special advisory committee status*.

While every association member participating in the HSCC maintains its own business-as-usual programs, the HSCC gives your organization visibility into other subsector perspectives and work initiatives, and a process-driven coordination mechanism to minimize conflict or duplication. **There are no membership dues to participate in the HSCC – only the contribution of your organization's available expertise, governance process, and programmatic**

reach in the development and implementation of policy and operational improvements to the security and resiliency of the sector.

The HSCC Cybersecurity Working Group. Over the past year, one component of the HSCC – the **Cybersecurity Working Group (CWG)** - has undertaken a number of important cybersecurity initiatives. Additional workstreams are expected to get underway for medical device and health IT security strategy and, more broadly, implementation of the Healthcare Industry Cybersecurity Task Force Report recommendations released in June 2017.

Call to Action. **The purpose of this message is a call to action to you and your membership.** As co-chairs of the HSCC Cyber Working Group, we observe that the sector's cybersecurity mission should be more robustly represented – both numerically and substantively -- across the six major subsectors: Direct Patient Care; Health Information Technology; Health Plans & Payers; Labs, Blood & Pharmaceuticals, Mass Fatality Management Services; and Medical Materials. Accordingly, we urge you to ensure that your organizations - representing critical service and technology providers with extensive economic concentration and population reach - are at the CWG table, providing expertise and resources to collaboratively address complex cybersecurity problems, and to partner with our government stakeholders in that process. We must operate under the principle that none of us individually is as smart as all of us collectively.

Hippocrates Initiative. We are now launching "Hippocrates" – our HSCC Cybersecurity Working Group acceleration initiative. As the father of modern medicine, Hippocrates did more than say "First, do no harm." He approached medicine with a rigorous, evidence-based discipline of diagnosis and care. This is the same method that drives our council work, and the malady is our collective "cyber insecurity" and its ultimate threat to patient safety, security and privacy.

Mark your calendars. Thus, ***we are calling an organizing meeting of the Healthcare Sector Council's Hippocrates Initiative for February 6, 2018 from 8:30am – 1:00pm*** (including a working lunch), and we strongly encourage you to attend and bring your horsepower. ***The meeting will be held at the U.S. Access Board, 1331 F Street, NW, downtown DC***. There, we will kick off Hippocrates with the following objectives:

- Convene national-level associations to significantly enhance membership numbers and representation at the HSCC CWG table
- Commit your associations' governing structures and member leadership to recruit the most influential and knowledgeable executives and subject matter experts to CWG liaison and leadership support. You must come to the table with your members' mindshare and authority to speak on their behalf according to your protocols
- Agree to a transparent and representational governance structure for the HSCC Cyber Working Group; and
- Coalesce around high-level cybersecurity and resilience principles around which we will organize task groups to accomplish collectively-prioritized objectives with measurable deliverables and outcomes

Then we will assemble the teams, elect our leaders and deliver what is expected of us – a more secure and healthier nation.

Who should attend. You can contribute any combination of skill sets to the Cyber Working Group including:

- CIO's, CISOs and their specialists
- Information and operational technology
- Legal counsel
- Government relations, and
- Risk and compliance.

Senior government officials to affirm the partnership. We will have with us at the start of this organizing meeting the HHS Assistant Secretary for Preparedness and Response, Robert Kadlec, and the Department of Homeland Security Assistant Secretary for Cybersecurity and Communications, Jeanette Manfra, to congratulate us on our renewed commitment and challenge us to deliver on our collective responsibility. They will then leave us to organize and work through our priorities and build the team.

We will send out to you shortly a calendar invitation, and more information about the agenda and expectations will follow. It is essential that your association and members are represented, and that you come prepared to take ownership of this responsibility and your leadership in it.

Attached is a powerpoint FAQ for additional background. Please direct questions to Executive Director Greg Garcia (greg.garcia@HealthSectorCouncil.org).

Who is invited so far. The table below lists 40 organizations so far receiving this invitation. We know there are many national associations with whom we have yet to reach out to, so we encourage you to make recommendations or introductions for such additions to Greg Garcia. After this organizational meeting we will work with you to launch successive rounds of membership development to recruit essential stakeholders across your association memberships.

Advanced Medical Technology Association	Aetna/NH-ISAC	Alliance for Nursing Informatics	America's Health Insurance Plans
American Association of Nurse Practitioners	American Health Care Association	American Health Information Management Association	American Hospital Association
American Medical Association	American Medical Group Association	American Medical Informatics Association	Association for Executives in Healthcare Information Security
Association for Healthcare Resource and Materials Management	Association for the Advancement of Medical Instrumentation	Biotechnology Innovation Organization	Blue Cross Blue Shield Association (BCBSA)
Center for Medical Interoperability	College of American Pathologists	College of Healthcare Information Management Executives	Cooperative Exchange/National Clearinghouse Association
Electronic Healthcare Network Accreditation Commission	Federation of American Hospitals	Healthcare Administrative Technology Association	Healthcare Industry Distributors Association
Healthcare Information & Management Systems Society	Healthcare Leadership Council	Healthcare Ready	HITRUST
Hospital Corporation of America	Medical Device Information Sharing and Analysis Organization	Medical Device Innovation Consortium	Medical Device Innovation Safety & Security Consortium
Medical Device Manufacturers Association	Medical Group Management Association	Medical Imaging Technology Association	National Association of Chain Drug Stores
NH-ISAC	PhRMA	Univ. Chicago Hospitals	Workgroup for Electronic Data Interchange

Attachment 3

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Healthcare Sector Coordinating Council Cybersecurity Working Group Membership Recruitment Meeting

February 6, 2018

SCC Co-Chairs

Dr. Bryan Cline, CISSP-ISSEP, CISM, CISA, CIPP/US
VP Standards & Analysis
HITRUST Alliance

Mr. Terrence (Terry) Rice
VP IT Risk Management & CISO
Merck & Co.

Executive Director
Greg Garcia

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

AGENDA

8:00 – 8:30 AM	Check-in, light continental breakfast
8:30 – 8:40	Leadership & Around-the-Room Introductions
8:40 – 9:10	Orientation about HSCC CWG Organization and Procedure
9:10 – 9:30	Q&A
9:30 – 9:50	Updates on Existing CWG Workstreams
9:50 – 10:00	Break
10:00 – 10:45	Jeanette Manfra, DHS Assistant Secretary for Cybersecurity & Communications Bob Kadlec, HHS Assistant Secretary for Preparedness & Response

AGENDA (CONT'D)

10:45 - Noon	**Work through Strawman Proposed Priority Initiatives** **<u>Objectives</u>:** - Breakout session to consider proposed initiatives and scope - Focus on cross-sector challenges - Add to and modify strawman as appropriate - Report out for purpose of agreeing on recommendations to full membership
12:00 – 12:15	**Grab lunch on premises**
12:15 -1:30pm	**Continue Priorities Discussion**
1:30 – (or earlier)	**Adjourn**

TODAY’S OBJECTIVES

- Member recruitment: Commitment from associations in attendance to join or to consider joining the CWG through their normal governance processes;
- Associations’ support for recruitment of their member hospitals, companies, clinicians and executives as new CWG members;
- Discussion about CWG governance structure and leadership; and
- A slate of new priority initiatives that can be forwarded as a recommendation to the existing full membership of the CWG.
- Attendees are being asked to come prepared to discuss these strawman initiatives and/or add new ones, whether or not specifically recommended in the June 2017 Cyber Task Force Report.
- Over the weeks following February 6, new initiatives will be vetted through the CWG membership for the purpose of agreeing to work plan and assigning task groups, leadership and volunteers to begin work streams to be defined by objective, deliverables, outcomes and timeline.

Notional CWG Calendar 2018

FEBRUARY 6	Associations organizing meeting - – agree on recommended initiatives for full CWG consideration
FEBRUARY 8	Initiative recommendations present at February 8 CWG meeting; comments solicited thru March 7
FEBRUARY 7 – MARCH 8	Associations aim for decision to join HSCC CWG, including task group membership and/ or leadership, by March 8 monthly CWG meeting; Recruit association members to join and to comment on initiatives
FEBRUARY 7 – MARCH 8	CWG meeting to approve initiatives slate; consider/elect task group leaders
MARCH 8	CWG meeting to approve initiatives slate; consider/elect task group leaders
MARCH 8 – forward	Solicit/recruit TG volunteers
MARCH 15	New Task Groups begin work; set deliverables, deadlines, and meeting schedule for year; New members welcomed ongoing
APRIL 12	Monthly CWG conference call; TG leads report initial progress
MAY 10	First full-in person CWG meeting for status and refinement of TG plans; followed by joint meeting with SSA, as appropriate. All-day combined
SEPTEMBER 13	Full CWG in-person status meeting, followed by Joint meeting with government partners (HHS, DHS); All day combined
THRU YEAR	CWG conference calls, webex's, etc., with HHS and separately, as needed

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTHCARE SECTOR COORDINATING COUNCIL

What Is It?

- The cross-sector coordinating body representing one of 16 critical infrastructure sectors identified in Presidential Executive Order (PPD-21)
- A trust-community partnership convening companies, non-profits and industry associations across six subsectors with HHS, DHS, law enforcement, and intelligence community
- ***Mission: to identify cyber and physical risks to the security and resiliency of the sector, and develop planning guidance in a 3-year Sector Specific Plan and implementing task groups for mitigating those risks***
- In meeting with government, it is the "Healthcare & Public Health SCC (HPH SCC")
- Focused on longer-term critical infrastructure policy and strategy, complementing the operational National Health Information Sharing and Analysis Center, which serves as the sector's tactical watch, warning, incident response, forensics, and best practices hub for intra-sector and government information sharing

HEALTHCARE SECTOR COORDINATING COUNCIL

How Does It Operate?

- Serves as a coordinating body – “the big table”- for industry associations and their members to unify effort toward policy and strategic solutions to shared security and resiliency challenges
- Does *not* supplant association work but coordinates their visibility, prioritization, and deconfliction
- Organized along functional and policy working groups with specific deliverables
- Regular meetings and conference calls and ongoing interaction with HHS as the principal sector specific agency (SSA)
- Forges joint work products – separately and with the government - that can be implemented across the sector to improve security and resiliency
- Strives to address *cross-cutting* issues affecting two or more subsectors, requiring industry associations and members to use their governing structures to enable accurate representation of their positions and agree to joint initiatives and outcomes

HEALTHCARE SECTOR COORDINATING COUNCIL

Who Is In It?

- The HSCC is composed of major stakeholders from the six HHS-identified sub-sectors - industry associations and their member organizations & individuals:
  - Direct Patient Care
  - Health Information and Medical Technology
  - Health Plans and Payers
  - Laboratories, Blood and Pharmaceuticals
  - Mass Fatality Management Services
  - Medical Materials
- Security vendors, consultants and service providers not specifically identified as critical healthcare infrastructure, or otherwise not uniquely essential to the support of healthcare service delivery, may contribute in an advisory capacity as requested by the membership, but not as voting members

HEALTHCARE SECTOR COORDINATING COUNCIL

How is the HSCC Different from a Trade Association?

- The HSCC is an *association of associations and their members*, with one unified focus: coordinated critical infrastructure protection (CIP) – both cyber and physical, working toward the common good
- As a recognized partner with the government under presidential executive orders (PPD 21 as amended), the HSCC-HHS ongoing partnership is given special protection from Freedom of Information Act exposure, per below
- To encourage and protect exchange of sensitive CIP information and planning, all SCC's – *not individual trade associations* – when collaborating with government are designated as "CIPACs" – Critical Infrastructure Protection Advisory Committees
- In order to maintain its CIPAC status, an SCC cannot directly lobby the way an association or company can
- **The SCC does not / cannot charge dues in order to retain its FOIA-exempt status when collaborating with government (dues are considered exclusionary)**

HEALTHCARE SECTOR COORDINATING COUNCIL

Why Participate in the HSCC?

- Collectively develop and implement policy and operational improvements to the security & resiliency of individual enterprises and the sector
- Build relationships and engage regularly with senior government officials in a trusted environment outside of – and protected from - any regulatory, public disclosure or competitive risks
- Gain visibility into other associations' initiatives and positions to deconflict and coordinate for efficient resource management and effectiveness
- Contribute to unity of effort as a counter-balance against regulatory or legislative intervention
- Demonstrate thought leadership toward the common good
- Step up to your organization's responsibility for the nation's public health and safety

HEALTHCARE SECTOR COORDINATING COUNCIL
CYBERSECURITY WORKING GROUP

What is the HSCC Cybersecurity Working Group?

- One of the standing Working Groups under the HSCC umbrella
- Tasked with identifying major cybersecurity threats and vulnerabilities to the security and resiliency of the healthcare sector, and developing cross-sector policy and strategic approaches to mitigating those risks

HEALTHCARE SECTOR COORDINATING COUNCIL
CYBERSECURITY WORKING GROUP

How is the HSCC Cybersecurity Working Group Currently Organized?

Current structure:

- Two-Co-Chairs: Terence Rice, Merck; Bryan Cline, HITRUST
- Six task groups (at different stages of progress, to be reassessed):
  - Future Gazing
  - Information Sharing
  - Risk Assessment
  - Risk Management
  - Communications and Marketing
  - 405(d) Implementation (Section 405d of 2015 Cybersecurity Act, requiring HHS to work with industry on cyber security standards of practice)

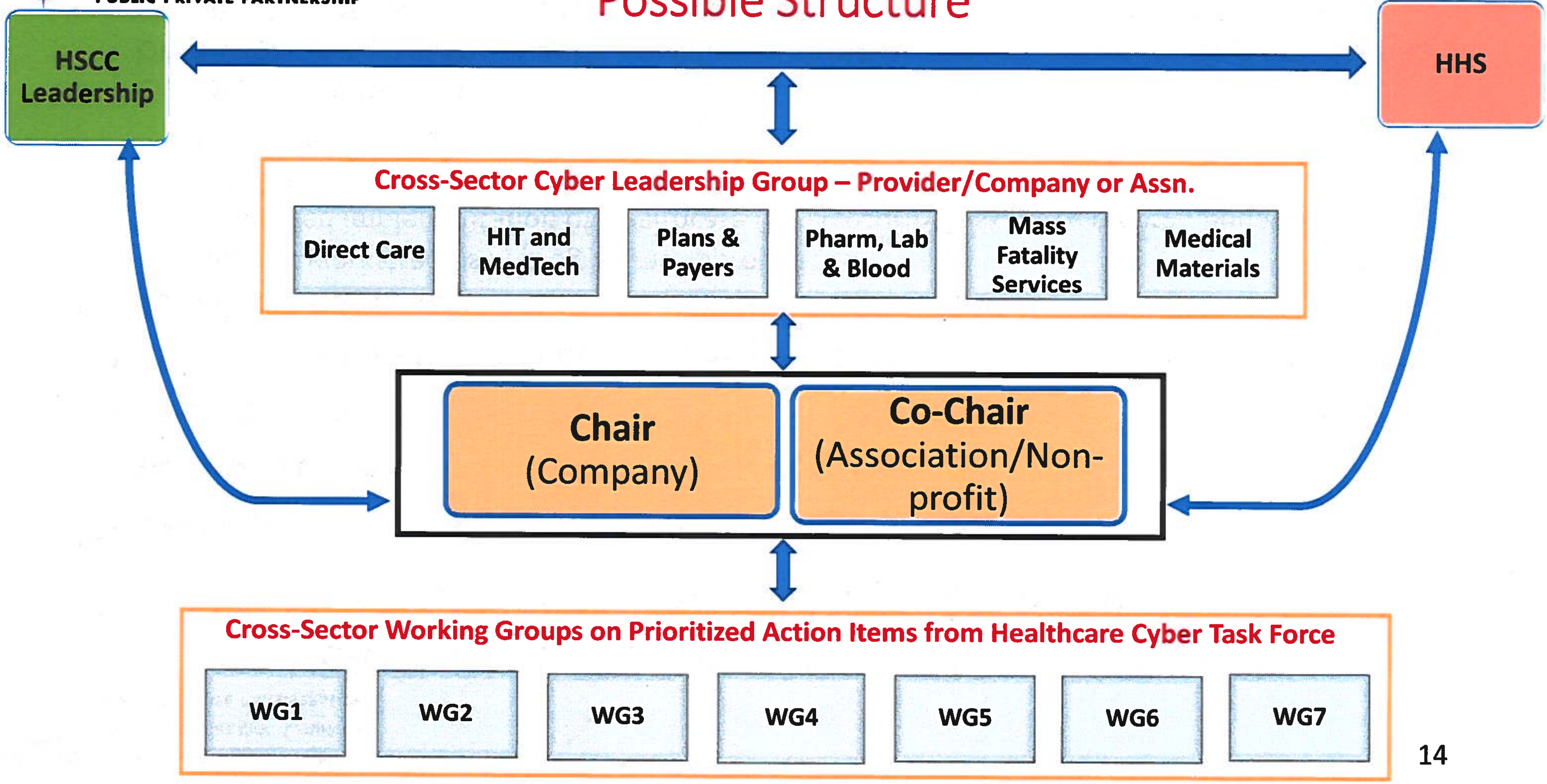
HEALTHCARE SECTOR COORDINATING COUNCIL
CYBERSECURITY WORKING GROUP

How Will the HSCC Cybersecurity WG Organization Evolve?

Proposed structure:

- Two-Co-Chairs
- Executive Committee comprising one from each of the six healthcare subsectors
- Task Groups focusing on specific deliverables to include:
  - Current workstreams in progress as appropriate
  - Prioritized implementation of Healthcare Cybersecurity Task Force recommendations
  - Medical Device Health IT Joint Strategic Plan
  - Others by consensus
- General membership of HSCC Cyber WG to include any and all association and organizational members with decision making authority, representing critical health subsectors, bringing technical, operational, management and public policy expertise to the table

Possible Structure


HSCC Leadership
HHS
Cross-Sector Cyber Leadership Group – Provider/Company or Assn.
Direct Care
HIT and MedTech
Plans & Payers
Pharm, Lab & Blood
Mass Fatality Services
Medical Materials
Chair (Company)
Co-Chair (Association/Non-profit)
Cross-Sector Working Groups on Prioritized Action Items from Healthcare Cyber Task Force
WG1
WG2
WG3
WG4
WG5
WG6
WG7

HEALTHCARE SECTOR COORDINATING COUNCIL
CYBERSECURITY WORKING GROUP

What Executive Roles are Required for Participation?

The Cybersecurity Working Group is composed of senior executives with decision-making authority from industry associations, healthcare enterprises and providers who have technical or managerial responsibility for:

- Cyber risk management
- Information and data management
- Information technology (IT) and operational technology (OT)
- Patient safety
- Product security
- Privacy and security compliance
- Policy, regulatory and legal affairs

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

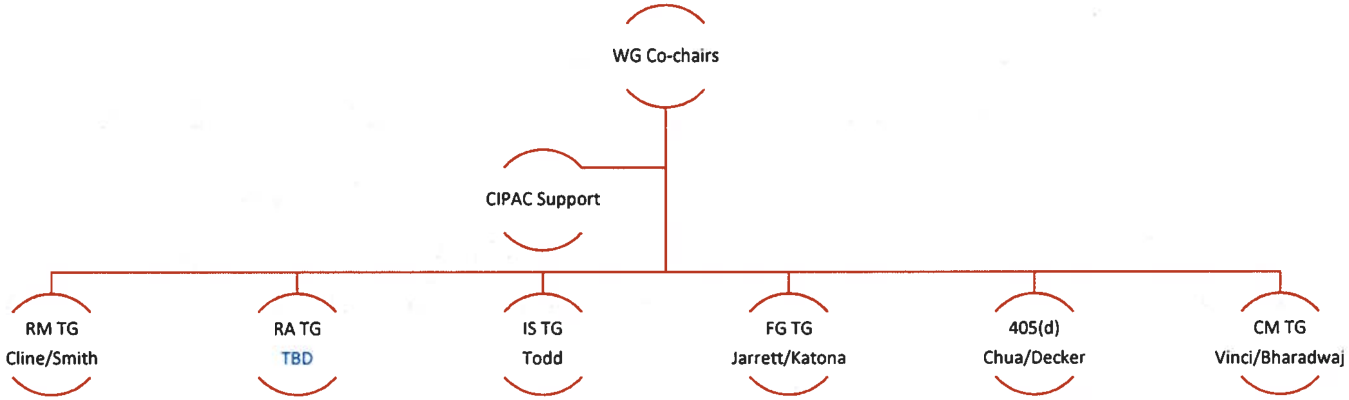
HEALTHCARE SECTOR COORDINATING COUNCIL

CYBERSECURITY WORKING GROUP

What is Ahead for the HSCC Cybersecurity Working Group?

- Expand membership from all six subsectors and essential industry associations
- New focus on prioritizing and implementing Healthcare Industry Cyber Security Task Force recommendations compiled under 6 Imperatives:
  1. Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity.
  2. Increase the security and resilience of medical devices and health IT
  3. Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
  4. Increase healthcare industry readiness through improved cybersecurity awareness and education
  5. Identify mechanisms to protect R&D efforts and intellectual property from attacks and exposure
  6. Improve information sharing of industry threats, risks, and mitigations

Task Groups



WG Co-chairs

CIPAC Support

RM TG
Cline/Smith

RA TG
TBD

IS TG
Todd

FG TG
Jarrett/Katona

405(d)
Chua/Decker

CM TG
Vinci/Bharadwaj

LEGEND

CIPAC – Critical Infrastructure Protection Advisory Council
CM TG – Communications and Marketing TG
FG TG – Future Gazing TG
IS TG – Information Sharing TG
RA TG – Risk Assessment TG
RM TG – Risk Management TG
TG – Task Group
WG – Working Group

Future Gazing TG (Jarrett/Katona)

- Members: Mark Jarrett, MD; Peter Katona, MD; Brian Quinn; Jay Kirkpatrick; Sanjeev Sah; Kelly Aldrich
- Deliverables: TBD
- Task: Develop an ongoing dialogue on how to incorporate new technology into healthcare and public health practice without compromising patient safety or access by individuals to their data as required by law
- Anticipated Products: Best practices submitted by members to include specific medical and IOT devices to be shared via a white paper or web posting
- Meeting Frequency: Monthly
- Next Meeting:
- Status:

Information Sharing TG (Todd)

- Members: Al Roeder; Bruce James; Connie Barrera; Ed Brennan; Greg Garcia; Lee Barrett; Michael Pry; Michael Vermilye; Nick Boukas; Nickol Todd; Tarik Rahmanovic; Terry Donat; Gary Fagan *(ADDITIONAL PARTICIPANTS WELCOMED)*
- Deliverables: TBD (See status)
- Task: Analyze existing and encourage new information-sharing activities regarding threat information, security incidents including exploits, breaches, and general cybersecurity information between government and private sector; develop or leverage existing timely, actionable incident management and cybersecurity alerts/guidance/best practices/educational materials, etc. for different types of audiences
- Anticipated Products: ISAO cyber security awareness within the HPH sector and support sector stakeholders to take action in response to CTI shared
- Meeting Frequency: Every 2nd Monday of the month @ 10:30am ET.
- Status:
- Review of HCIC Task Force recommendations on information sharing completed; most critical identified as:
  - **Action Item 6.1.1** - HHS / Information Sharing and Analysis Organizations (ISAOs) should streamline and consolidate information sharing data on threats whenever practical for easier consumer adoption
  - **Action Item 6.3.3** - HHS, DHS NCCIC, and law enforcement should maintain unified and dedicated channels during steady state and response efforts to provide SME support, leveraging existing relationships and facilitate targeted dissemination …
  - **Action Item 6.2.2** - HHS / fed partners should ensure intelligence reports and threat information is consolidated and given additional context as distributed industry
- Comments on draft *Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats* are due February 12, 2018

Risk Assessment TG (TBD)

- Members: TBD
- Deliverables: Whitepapers/recommendations for addressing HPH sector gaps in cybersecurity risk assessment (analysis); may be incorporated into the sector guide
- Task: Support development of the HPH Sector Risk Assessment Tool
- Anticipate Products: Cybersecurity questions in the HPH Sector Risk Assessment Tool to be released to the public in FY18
- Meeting Frequency: TBD
- Next Meeting: TBD
- Status: TBD

Risk Management TG (Cline/Smith)

- Members: Damon Becknel, Thomas Byrd, Dr. Seth Carmody, Aaron Clegg, Dr. Claude (Chip) Council, Leo Dittemore, Sara DuVall, Anna Etherton, Dr. Cris Ewell, Dr. Julian Goldman, Daryl Hykel, Noah Jaehnert, Marilyn Zigmund Luke, David Muntz, John Overbaugh, Ramakrishnan Pillai, Clay Ramsey, Munzoor Shaikh, Nick (James) Sloan, Mike Von Hoven, Peter Walker, David Wiseman
- Task: Coordinate the development of a tailored, Sector-wide HPH Implementation Guide of the NIST Cybersecurity Framework, leveraging existing documents and efforts within and beyond GCC/SCC partners, and develop supplemental guides that are tailored to different levels of users
- Updates to the 2016 Healthcare Sector Cybersecurity Framework Implementation Guide, including but not limited to new content around small business and cloud security
- Deliverables: Formal HPH sector-specific guidance on implementing the NIST CsF (*Healthcare Sector Cybersecurity Framework Implementation Guide*)
- Meeting Frequency: Every 4th Thursday of the month @ 1 PM CT
- Next meeting: 21 Jan 2018
- Status: *See next slide*

Current V2 Production Status (1)

Task Name Task Description	Priority	Status
Body – General	**Low**	🟧 **0%**
Explain how any control framework (e.g., ISO) can be used in approach; update resources to include new NIST-Baldridge Cyber Assessment Tool		
App. F – NIST CsF and HIPAA Security Rule Mapping	**Medium**	🟥 **20%**
Update OCR crosswalk with RM SG recommended mappings		
App. H – Cybersecurity Preparedness Model (CPM)	**Medium**	🟩 **75%**
Incorporate Intel's high-level maturity assessment/model; flesh out existing preparedness model		
App. I – Small Organization Implementation Guidance	**High**	🟩 **75%**
Provide "good hygiene" approach to cybersecurity for smaller, lower risk organizations		
App. J – Cybersecurity Program Policy Guidance	**Low**	🟧 **10%**
Describe approach to policy development based on HPH sector guidance for NIST CsF implementation		
App. K – Executive Marketing / Summary Template	**Medium**	🟧 **40%**
Provide sample presentation advocating benefits of the NIST CsF and HPH sector approach / guidance		

Legend: % - Estimated Work Complete; R/Y/G – High/Medium/Low Risk of Not Completing the Deliverable In Time for a 1 Apr 2018 Draft

Current V2 Production Status (2)

Task Name Task Description	Priority	Status
App. L – Healthcare CsF Structure	**Medium**	🟩 40%
Brief discussion of how the HITRUST CSF and NIST CsF fit together; with graphics		
App. M – Corrective Action Plan (CAP) Example	**Medium**	🟩 60%
Provide a brief overview along with several examples of various CAPs		
App. N – Communications Plan Template	**High**	🟧 **40%**
PMI-like communications plan for implementation of the NIST CsF using the HPH sector guidance		
App. O – Medical Device Security (MDS)	**High**	🟩 50%
Discussion of MDS issues, available resources, when to use them, and how they support the NIST CsF		
App. P – Industry Resources Mappings	**High**	🟧 **0%**
High-level mappings of industry resources to the NIST CsF (similar to other sector guides)		
App. Q – Cloud-based Services	**High**	🟩 60%
Discussion of Cloud-based service security issues and recommended controls for Cloud Service Providers		

Legend: % - Estimated Work Complete; R/Y/G – High/Medium/Low Risk of Not Completing the Deliverable In Time for a 1 Apr 2018 Draft

Current V2 Production Status (3)

Task Name Task Description	Priority	Status
App. R – Frequently Asked Questions (FAQs)	**Low**	🟩 100%
Various FAQs and associated responses		
App. S – PMI Organization Implementation Guidance	**Low**	**50%**
A review of current PMI-specific guidance for implementation of the NIST CsF		
App. T – Executive Dashboards	**Medium**	🟩 75%
Guidance on executive-level dashboarding with examples		

Legend: % - Estimated Work Complete; R/Y/G – High/Medium/Low Risk of Not Completing the Deliverable In Time for a 1 Apr 2018 Draft

Comm. & Marketing TG (Vinci/Bharadwaj)

- Members: Esther Lawson; Drew Williams; David Muntz; Jason Smith
- Task: Facilitate internal communications to support the work of the Working Group and external marketing to facilitate the communication of the Working Groups deliverables to the broader HPH Sector
- Anticipated Products: Web platforms (e.g., SharePoint, Wikis), press releases, articles, conference presentations and other forms of communication that will promote awareness of the WG's activities and work products
- Meeting Frequency: Monthly
- Next Meeting:
- Status: Recruiting; The TG did not meet over the holidays and will provide an update at the 8 Feb Joint CWG meeting

CISA 405d Task Group (Erik Decker – Julie Chua)

- Members: Julie Chua; Erik Decker ~110 total; 50 regularly participating industry members

From CISA 405(d) "a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes"

- Meeting Frequency: ~Monthly interaction with the Task Group
- Next Meeting: Writing Committee meets weekly, teams bi-weekly, full Task Group again at end of March
- Status: Writing

Industry-Led Activity to Improve HPH Cybersecurity

WHAT IS THE 405(d) EFFORT?

An industry-led process to develop consensus-based guidelines, best practices, & methodologies to strengthen the HPH-sector's cybersecurity posture

HOW WILL 405(d) ADDRESS HPH CYBERSECURITY NEEDS?

With a targeted set of applicable & voluntary guidance that seeks to cost-effectively reduce the cybersecurity risks of healthcare providers

WHO IS PARTICIPATING?

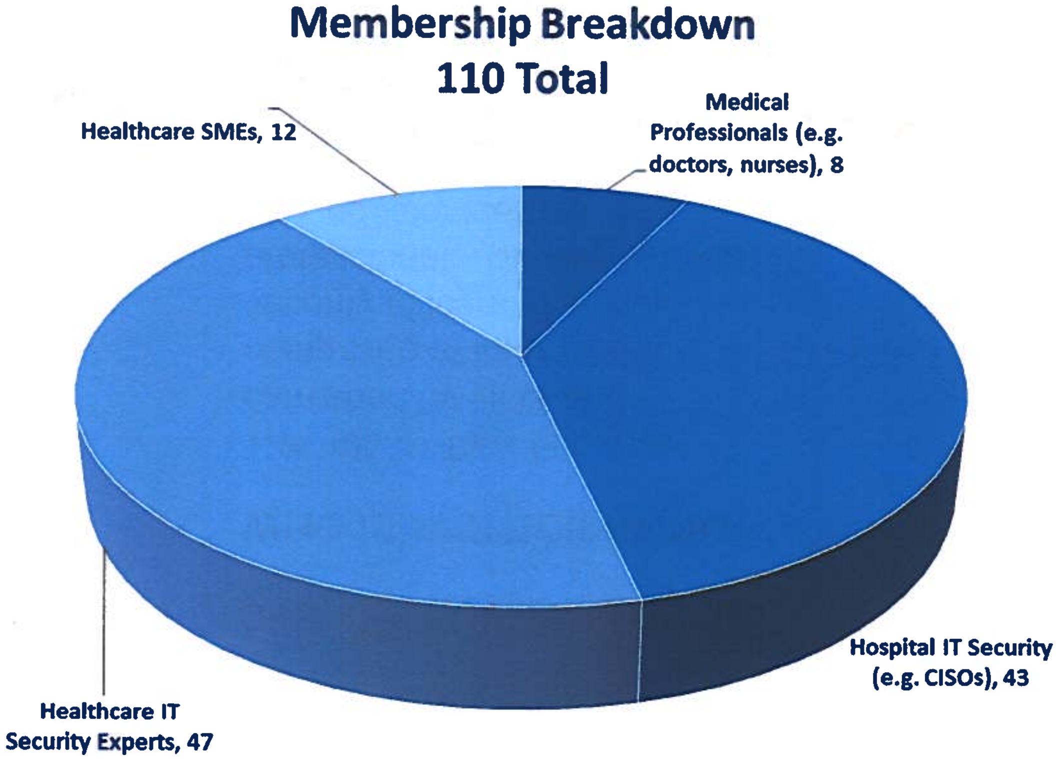
The 405(d) Task Group is convened by HHS and comprised of information security officers, medical professionals, privacy experts, and industry leaders

WHY IS HHS CONVENING THIS EFFORT?

Congress mandated the effort in the Cybersecurity Information Sharing Act of 2015 (CISA) Section 405(d): Aligning Health Care Industry Security Approaches

405d Task Group

Note: At its inception, the 405d Task Group call to action leveraged the GCC and SCC list and some existing relationships with industry stakeholders for initial membership.



What Does the Industry Task Group Want to Produce?

ACTIONABLE AND EASY TO USE BEST PRACTICES

INDUSTRY-LED, CONSENSUS & VOLUNTARY

CHARACTERISTICS

PRACTICAL AND EASY TO UNDERSTAND

SCALABLE & RELEVANT TO HEALTHCARE PROVIDERS OF EVERY SIZE AND RESOURCE LEVEL

BETTER INFORMED HPH SECTOR

VETTED BEST PRACTICES FOR DIFFERENT SIZED ORGANIZATIONS

BENEFITS

FOSTERING CONSISTENCY

KNOWING “WHAT TO ASK”, “WHEN TO ASK”, AND “WHO TO ASK”

405(d): Timeline

Stage One: “Foundation”	• **May 22-23 2017**: Session #1 (In-Person) • **June 26 2017**: Session #2 (WebEx) • **July 17-18 2017**: Session #3 (In-Person)
Stage Two: “How-To”/Subgroups	• **August 2017 – Early September 2017**: Subgroups Convene and Address “Annotated Outline” and Topics
Stage Three: “Assessment”	• **September 18-19 2017**: Session #4 (In-Person) • **October 2017 – December 2017**: 1. After Action Review (October) 2. Peer Review Roundtables (November) 3. Session #5 WebEx Sessions (mid-December)

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

405(d): Where are We?

Stage Four: "Initial Document"	• **Early 2018:** 1. Writing Committee & First Draft of Version 1.0 of Guidance **|| Targeting a Mid-February Draft | |** 2. Session #6 on March 26-27 (Task Group ratification of First Draft of Version 1.0)
Stage Five: "Pre-Testing"	• **Spring 2018 – Fall 2018**: *Assessing the Output*: Nationwide Pre-Testing with Healthcare Professionals (Tentative: 10-15 cities)

- **Next Stages || Sustained Engagement: Mid-2018**: Integrating Feedback, Informing and Educating, Moving to V2.0

Pre-testing the 405(d) Guidance

How Can We Leverage Existing Relationships With National/Regional Associations Through the SCC?

- Stakeholder research indicates that local affiliates/members of national/regional associations are the best "force multipliers" to assemble groups for 405(d) pretests.
- Work with the local affiliates, in coordination with and/or through their national/regional offices, to identify medical providers and hospitals that are willing to participate in and host pretesting of voluntary cybersecurity guidance.
- **Pretesting will help us understand if the guidance is usable, actionable, practical, and scalable before it is finalized and released publicly.**
- Introducing staff at the working level – association staff to 405(d) support team so work can begin.

How do I get Involved?

- For more information, send an email to CISA405d@hhs.gov

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Medical Device & Healthcare IT Cybersecurity Framework and Joint Strategic Plan

Healthcare Cybersecurity Learns From Others

Montreal Protocol improving the ozone layer:

- Goal of phasing out ozone-depleting chemicals, including chlorofluorocarbons (CFCs); once widely used in refrigerators and spray cans.
- Outlined framework to replace CFCs with HFCs and later amended to phase out HFCs
- Agreement from 197 countries to meet key milestones with phase out levels and to promote business with agreement members

Healthcare industry can take similar action:

- Goal of phasing out legacy and EOL healthcare technology that lack security controls
- Outline framework for replacing legacy Healthcare Technology with ones that adhere to certain risk management and technical standards in Healthcare Provider environments that adhere to standards
- Agreement from Healthcare Providers and Vendors to meet key milestones with maturity and promote business with those participants

Introduction to MD-HIT CSF and JSP

Objectives: Establish a voluntary framework and joint strategic plan for medical devices and healthcare information technology cybersecurity which outlines how to achieve the following:

- Address risk of end-of-life and legacy products
- Promote transparency on security and its relation to patient safety for products
- Provide consistent secure product development practices
- Clarify vulnerability communication and incident response coordination
- Assess maturity and establish milestones for achieving success
- Create governance structure for continuous improvement

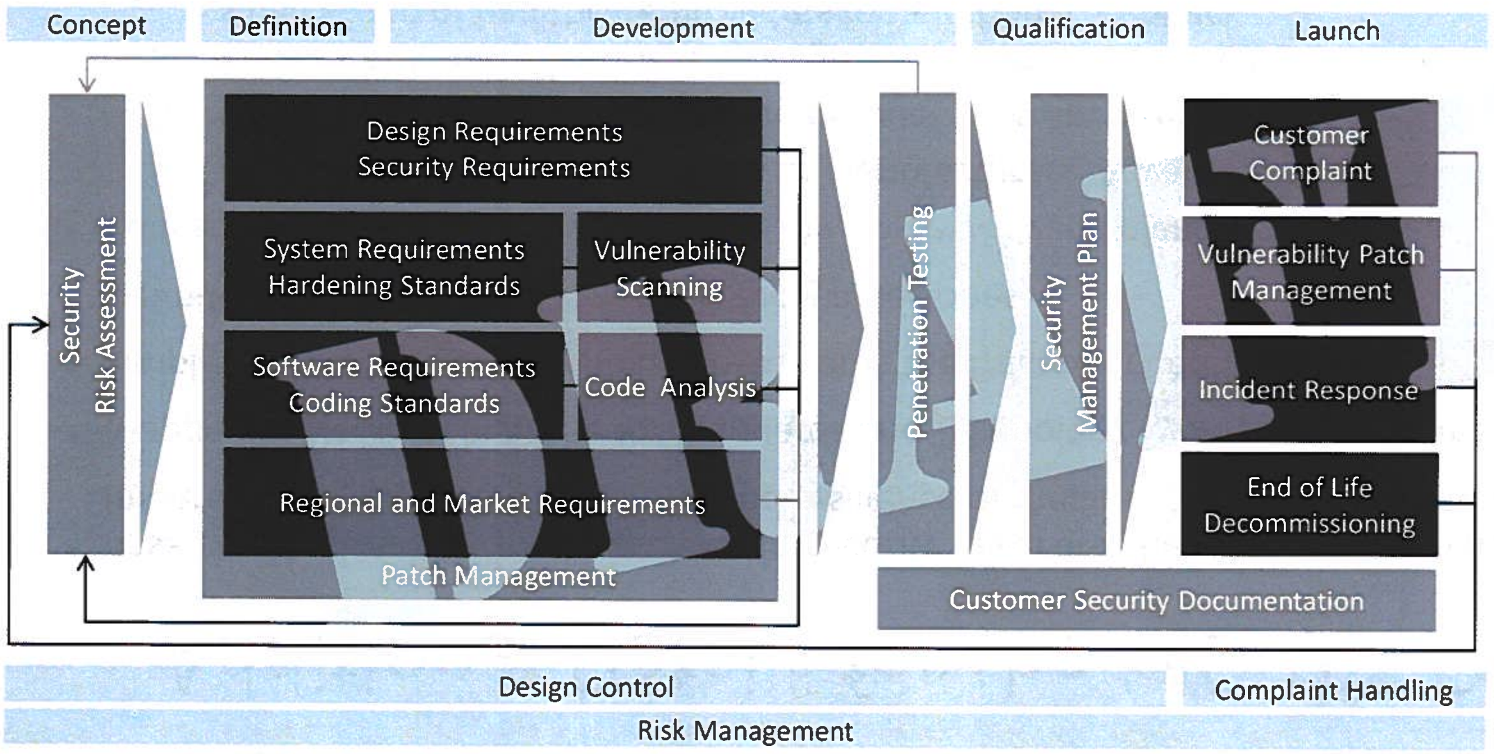
Participants: Medical Device Manufacturers, Healthcare IT Vendors, Healthcare Providers, Trade Associations, Federal Agencies, Standards Organizations, and Security Technology and Research

Additional Details for the MD-HIT CSF and JSP

- Based on the Health Care Industry Cybersecurity Task Force Report recommendations within Imperative 2 “Increase the security and resilience of medical devices and health IT”
- Mapped to National Institute for Standards and Technology Cybersecurity Framework
- Simple criteria for assessing maturity towards the framework and plan
- Definition of responsibilities for achieving milestones
- Consensus-based approach to drafting the framework and plans includes:
  1. Draft the JSP with a small group of manufacturers, AdvaMed, and FDA
  2. Present and solicit feedback from broader manufacturer group
  3. Present and solicit feedback through FDA, AdvaMed, MITA, MDMA, CHIME, MedISAO to a small group of healthcare providers for additional feedback
  4. Through the Healthcare SCC perform industry review and establish a governance model to ensure baseline strategy is routinely updated

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Example of the MD-HIT CSF and JSP



- Coordinated Disclosure in 30 days via ICS-CERT by May 2019

- Code Analysis and Secure Coding Standards in QMS by March 2018

- Customer Security Documentation by September 2020

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Thank you!

DHS Assistant Secretary for Cybersecurity and Communications Jeanette Manfra

HHS Assistant Secretary for Preparedness and Response Robert Kadlec

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT.
3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4. Increase health care industry readiness through improved cybersecurity awareness and education.
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.
6. Improve information sharing of industry threats, risks, and mitigations.

BREAKOUT QUESTIONS
FROM INITIATIVES STRAWMAN

- What is missing?
- Which are most important?
  (short/mid/long term priorities)
- Which require special or additional resources
- Which will your organization participate in?

Attachment 4

HEALTHCARE
LEADERSHIP
COUNCIL

February 16, 2018

Don Rucker, M.D.
National Coordinator for Health Information Technology
Department of Health and Human Services
330 C St. SW Floor 7
Washington, D.C. 20201

Dear Dr. Rucker:

The Healthcare Leadership Council (HLC), a group of leaders across all sectors of American healthcare, appreciates the opportunity to comment on the Trusted Exchange Framework and Common Agreement (TEFCA) released by the Office of National Coordinator (ONC). We applaud the vision of this framework and ONC's leadership on advancing interoperability.

HLC is a coalition of chief executives from all disciplines within American healthcare. It is the exclusive forum for the nation's healthcare leaders to jointly develop policies, plans, and programs to achieve their vision of a 21st century health system that makes affordable, high-quality care accessible to all Americans. Members of HLC – hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors, pharmacies, post-acute care providers, and information technology companies – advocate for measures to increase the quality and efficiency of healthcare through a patient-centered approach.

The Healthcare Leadership Council supports ONC's intent to advance interoperability to increase access to health information between and among patients, payers and providers, irrespective of location, to provide a longitudinal health record and deliver high quality care. We commend the concepts and precepts of this effort. HLC has questions, however, about how the entities established and participating in this framework will transfer and deliver health information to all stakeholders across the continuum of care.

HLC seeks clarification surrounding the Recognized Coordinating Entity (RCE), its implementation of the common agreement and the way in which it will operationalize the Trusted Exchange's Framework. HLC also seeks clarification on the framework's relationship to HIPAA, as well as, more clarity surrounding stakeholder participation in the framework. There is considerable detail in the appended documents to the TEFCA framework but clarifying these areas to avoid complications as implementation occurs will be helpful.

HLC also recommends that the ONC synchronize definitions and terms across TEFCA and US Core Data for Interoperability documents (USDCI). More specifically, we respectfully request that ONC consider connecting various features across TEFCA and USDCI development, namely, the implementation of application programing interfaces (API's), interoperability standards, the definition of what 'open API' really means as requested in the 21st Century Cures Act, the semantic standards for electronic health records (EHR's) reporting and data transfer, and clear distinctions between business and political based information blocking and technical impediments to database access and understanding due to terminology ambiguity. Lastly, we seek greater clarity related to patient matching, user identity authentication, user cases, permitted purposes and queries.

Specifically, we seek answers from ONC to the following questions:

RCE/Common Agreement

- How will the RCE be structured? What are the roles and responsibilities of the RCE? We recommend that the RCE should be neutral, transparent, and objective as it governs a network of QHINs (Qualified Health Information Network). The governing board should be balanced so that all stakeholders are adequately represented.
- How much funding will be allocated to the RCE?
- What barriers will the RCE and common agreements address?
- How was the analysis conducted to assess current regulatory authority and legal standards? How does this analysis enable and promote interoperability?
- What are the details of the common agreement and how will it be developed?
- There is clearly a need for standardization to which all participating entities should adhere; How does ONC plan to address, certify and monitor use of such standards?
- We are generally supportive of the requirements for the QHIN. We recommend that ONC define the functional requirements for a QHIN and allow the neutral-bodied RCE and QHINs to define the technical requirements.

HIPAA

- Does participation by non-HIPAA covered entities require them to be covered under HIPAA in the TEFCA framework?
- How does the TEFCA framework handle data requests that do not fall under HIPAA?
- Who will manage consent under the TEFCA model?
- How will ONC work with industry to ensure the accounting of disclosures requirement under TEFCA is realistically feasible for industry? (HLC strongly opposes the access report provision of the HIPAA Accounting of Disclosures NPRM 76 FR 31426).

Participants/Stakeholders

- What are the overall costs to those who participate? We recommend that attributable costs be driven by market factors and not regulated by ONC through TEFCA.
- What are the fees and fee structures for services?
- Will stakeholders need to make substantial investments in infrastructure and in changes/upgrades?
- What is the likelihood federal agencies will require TEFCA participation?
- Is it reasonable to expect participants to ensure every patient's medications and medical information are up to date prior to data exchange with other organizations?
- What incentives for participation can be provided? History has shown that the business model for wide-ranging health exchange networks is challenging, and while ethically and morally the right thing to do, such network unification, maintenance is often not fiscally rewarding enough to encourage participation.

Other general questions:

- How do new regulations related to medical devices in information technology, such as US Device Innovation (USDI), fit within the TEFCA framework?
- How does the Unique Device Identifier (UDI) relate (or not) to other existing and in process data model efforts?
- Does ONC believe previous experience is sufficient to suggest TEFCA will be successfully scaled, or should consideration be given to conducting a pilot study to determine scalability?
- Should ONC collaborate with the National Institutes of Standards and Technology (NIST) and RCE to design a pilot program, with the pilots completed before TEFCA is finalized?
- Individuals who previously agreed to share information via the framework may withdraw their consent in the broader contextual effort, and if an individual decides to cease sharing information, how will the data already shared across all networks be affected?
- Lastly, how will the framework impact value-based care initiatives and the Merit-based Incentive Payment System (MIPS) program?

The Healthcare Leadership Council believes the Trusted Exchange Framework and Common Agreement will help to build a solid foundation to increase access to health information and improve communication among all stakeholders within healthcare. We applaud the intent of ONC to produce a framework aimed at supporting interoperability and increasing the flow of information among interrelated healthcare entities, and we respectfully request ONC consider our questions and suggestions to improve upon the framework's foundation. HLC stands ready to assist ONC with an approach to increasing access to healthcare information across all stakeholders. Should you have any questions, please do not hesitate to contact Tina Grande at (202) 449-3433 or tgrande@hlc.org.

Sincerely,

Mary R. Grealy

Mary R. Grealy
President

Attachment 5

CONFIDENTIALITY
COALITION

February 20, 2018

The Honorable Lamar Alexander
Chairman
U.S. Senate Committee on
Health, Education, Labor & Pensions
428 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Patty Murray
Ranking Member
U.S. Senate Committee on
Health, Education, Labor & Pensions
428 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Alexander and Ranking Member Murray,

The Confidentiality Coalition is writing to you to urge passage of S. 1850, Protecting Jessica Grubb's Legacy Act, to enable the appropriate exchange of necessary information among medical professionals who are treating individuals with substance use disorders, including opioid abuse. While the Confidentiality Coalition commends the U.S. Substance Abuse and Mental Health Service Administration's (SAMHSA's) ruling to amend 42 C.F.R. Part 2 to better align Part 2 regulations within the Health Insurance Portability and Accountability Act (HIPAA) to integrate behavioral and physical healthcare, we believe this ruling does not go far enough to help increase access to relevant health information among patients, payers and providers while concurrently protecting patient privacy.

The Confidentiality Coalition is a broad group of organizations spanning all sectors of healthcare working to ensure that policies are implemented to appropriately balance the protection of confidential health information with the efficient and interoperable systems needed to provide high quality healthcare. Access to timely and accurate patient information leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

The Confidentiality Coalition is comprised of hospitals, medical teaching colleges, health plans, pharmacies, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacy benefit managers, health information and research organizations, clinical laboratories, and others. Through this diversity, we develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers.

Current federal regulations governing the confidentiality of drug and alcohol treatment and prevention records (42.C.F.R. Part 2 (Part 2)) preclude the Centers for Medicare & Medicaid Services (CMS) from disclosing medical information to healthcare providers for care coordination, including those engaged in accountable care organizations and bundled payment organizations. These regulations currently require complex and multiple patient consents for the use and disclosure of patients' substance use records that go beyond the sufficiently strong patient confidentiality protections that were subsequently put in place by HIPAA.

Electronic health records and value-based payment models such as Accountable Care Organizations (ACOs), Health Information Exchanges (HIEs), Medicaid Health Homes and related Medicare and Medicaid integrated care programs were designed to create a more holistic, patient-centered approach to healthcare where providers work together to coordinate across their traditional silos and in some cases are held jointly accountable for the quality, outcomes and cost of that care. Critical to making these new models work for patients is having access to the individuals' health records, including those related to substance use disorders. CMS provides participating providers of Medicare ACO and bundled payment organizations with monthly Medicare Parts A, B and D claims under data use agreements that include criminal penalties for misuse. Yet, due to outdated laws mentioned above, CMS is forced to remove *all* claims where substance use disorder is a primary or secondary diagnosis. Patient safety is also threatened with the potential pharmaceutical contraindications that could occur without access to the full medical record. Without this critical information, providers are prevented from understanding the full extent of their patients' medical needs.

We commend SAMHSA's recent rule making efforts, and understand the agency has probably gone as far as possible in regards to attempts to modernize the Part 2 Rule. To sufficiently address the need for further reform, Senator Joe Manchin (D-WV) introduced S. 1850 to ensure healthcare providers have access to the full medical record, including information on substance use disorders, to effectively and safely treat patients suffering from substance use disorders while guaranteeing the privacy and security of substance use medical records. In particular, S.1850 would reinforce and expand existing prohibitions on the use of these records in criminal proceedings.

We urge the Committee to consider S. 1850 to amend 42 CFR Part 2 and align with HIPAA's treatment, healthcare operations and payment policy as one of several potential solutions Congress passes to help with the opioid crisis. Thank you for your attention to this important matter.

Sincerely,

Tina Grande

Tina O. Grande

Tina Grande
Healthcare Leadership Council on behalf of the Confidentiality Coalition

Attachment 6

CONFIDENTIALITY
COALITION

February 20, 2018

The Honorable Greg Walden
Chairman
U.S. House of Representatives
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone
Ranking Member
U.S. House of Representatives
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Walden and Ranking Member Pallone,

The Confidentiality Coalition is writing to you to urge passage of H.R. 3545, the Overdose Prevention and Patient Safety (OPPS) Act, to enable the appropriate exchange of necessary information among medical professionals who are treating individuals with substance use disorders, including opioid abuse. While the Confidentiality Coalition commends the U.S. Substance Abuse and Mental Health Service Administration's (SAMHSA's) ruling to amend 42 C.F.R. Part 2 to better align Part 2 regulations within the Health Insurance Portability and Accountability Act (HIPAA) to integrate behavioral and physical healthcare, we believe this ruling does not go far enough to help increase access to relevant health information among patients, payers and providers while concurrently protecting patient privacy.

The Confidentiality Coalition is a broad group of organizations spanning all sectors of healthcare working to ensure that policies are implemented to appropriately balance the protection of confidential health information with the efficient and interoperable systems needed to provide high quality healthcare. Access to timely and accurate patient information leads to both improvements in quality and safety and the development of new lifesaving and life-enhancing medical interventions.

The Confidentiality Coalition is comprised of hospitals, medical teaching colleges, health plans, pharmacies, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacy benefit managers, health information and research organizations, clinical laboratories, and others. Through this diversity, we develop a nuanced perspective on the impact of any legislation or regulation affecting the privacy and security of health consumers.

Current federal regulations governing the confidentiality of drug and alcohol treatment and prevention records (42.C.F.R. Part 2 (Part 2)) preclude the Centers for Medicare & Medicaid Services (CMS) from disclosing medical information to healthcare providers for care coordination, including those engaged in accountable care organizations and bundled payment organizations. These regulations currently require complex and multiple patient consents for the use and disclosure of patients' substance use records that go beyond the sufficiently strong patient confidentiality protections that were subsequently put in place by HIPAA.

Electronic health records and value-based payment models such as Accountable Care Organizations (ACOs), Health Information Exchanges (HIEs), Medicaid Health Homes and related Medicare and Medicaid integrated care programs were designed to create a more holistic, patient-centered approach to healthcare where providers work together to coordinate across their traditional silos and in some cases are held jointly accountable for the quality, outcomes and cost of that care. Critical to making these new models work for patients is having access to the individuals' health records, including those related to substance use disorders. CMS provides participating providers of Medicare ACO and bundled payment organizations with monthly Medicare Parts A, B and D claims under data use agreements that include criminal penalties for misuse. Yet, due to outdated laws mentioned above, CMS is forced to remove *all* claims where substance use disorder is a primary or secondary diagnosis. Patient safety is also threatened with the potential pharmaceutical contraindications that could occur without access to the full medical record. Without this critical information, providers are prevented from understanding the full extent of their patients' medical needs.

We commend SAMHSA's recent rule making efforts, and understand the agency has probably gone as far as possible in regards to attempts to modernize the Part 2 Rule. To sufficiently address the need for further reform, Representatives Markwayne Mullin and Earl Blumenauer have introduced H.R. 3545 to ensure healthcare providers have access to the full medical record, including information on substance use disorders, to effectively and safely treat patients suffering from substance use disorders while guaranteeing the privacy and security of substance use medical records. In particular, H.R. 3545 would reinforce and expand existing prohibitions on the use of these records in criminal proceedings.

We urge the Committee to consider H.R. 3545 to amend 42 CFR Part 2 and align with HIPAA's treatment, healthcare operations and payment policy as one of several potential solutions Congress passes to help with the opioid crisis. Thank you for your attention to this important matter.

Sincerely,

Tina Grande

Tina O. Grande

Tina Grande
Healthcare Leadership Council on behalf of the Confidentiality Coalition

cc: U.S. House of Representatives