National Committee on Vital and Health Statistics
Advising the HHS Secretary on National Health Information Policy

PSC Subcommittee Update: Virtual Hearing on Security in Healthcare

NCVHS Subcommittee on Privacy, Confidentiality and Security

September 9, 2021

Today's agenda

- Review of Hearing and Major Themes
- Review of Next Steps from Project Scope
- Timeline
- Discussion

Security Hearing: Panel 1

Panel 1: Addressing Healthcare Security Challenges

Panelists:

- Jane Wong, Chief Information Officer of UCSF Health, and Sabrina Kidd, Chief Medical Officer, UCSF Health
- Erik Decker; Assistant Vice President/Chief Information Security Officer, Intermountain Healthcare
- Denise Anderson, President of H-ISAC

Major Themes from Panel 1

- The need for sharing/coordination of best practices for cybersecurity
- Increased awareness of H.R. 7898 (Public Law 116-321)
- Fewer penalties/more incentives for cybersecurity
- Sharing of threat information, and understanding of how to do so
- Need for a playbook of top 20 things to do for cybersecurity response
- Lack of expertise in cybersecurity in health
- Thin margins in healthcare, less for cybersecurity

Top Priorities from Panel 1

- Playbook that could be shared
- More accountability for vendors on security updates e.g., Patching requirements
- More support within the operations division that represents the sector risk management agency. ASPR only had 1-1.25 FTEs. If we had more dedicated support, we could do more if they coordinated among FDA, CMS, CDC, etc.
- Implementation of PL 116-331, bypass the RFI and go directly to NPRM would be great so as not to cause delay, people are waiting to see what OCR will do to implement the law
- More coordination/collaborating when incidents happen.

Security Hearing: Panel 2

Panel 2: State, Tribal and other Perspectives on Healthcare Security

Panelists:

- John Guerriero, Cybersecurity Program Director – Acting, National Governors Association
- Kevin Fu; Acting Director, Medical Device Cybersecurity and Program Director for Cybersecurity, Digital Health Center of Excellence, FDA

Major Themes from Panel 2

- Priority areas: cyber governance, critical infrastructure, workforce development, response planning
- How to deal with legacy systems at state level: this is something many are struggling with
- Examining the risks for organizations sharing threat information

Priorities from Panel 2

- Public health should have a seat at the table for newly designed Cyber Safety Review Board under EO. Equivalent to NTSB.
- Need help with legacy technology including financial support. Public health and healthcare organizations are struggling with upgrading or securing legacy systems.
- More information sharing on threats including the risks and remediation recommendations.

Security Hearing: Panel 3

Panel 3 — Emerging Security Threats and Preparedness Across the Healthcare Industry

Panelists:

- Suzanne Widup; Senior Analyst, Verizon Enterprise Solutions
- Kevin Stine; Chief of the Applied Cybersecurity Division in the NIST's Information Technology Laboratory (ITL)

Major Themes from Panel 3

- Need to adopt practices to make data less vulnerable
- Ransomware is 10% of breaches. This is a major change.
- Cloud assets are attacked more often than on-premises resources. Data is more accessible in the cloud.
- Breaches are more often outsiders, motivated by financials. Criminals will follow money wherever it goes.
- Rise in social engineering attacks
- Privilege misuse is common in health care (malicious insiders, using access granted for job to do something else – snooping, or stealing data to monetize in some form). These incidents are more difficult to detect because they are done by employees with authorization.

Major Themes from Panel 3, cont.

- Opportunities for outreach, not just putting out documents: videos, infographics, cheat sheets, quick start guides, help to meet people and orgs where they are.
- Ransomware is a “service” – there is a market for malicious capabilities, looking at the research opportunities to begin to have the guidelines and standards
- Security is not one size; risk based so it should be tailored to each organization’s own environment.
- Detection and response need to be prioritized
- Incident response plans are key.
- Cyber is not a problem to be solved but managed. Ultimately it is a risk management issue for every organization: large/small public/private

Priorities from Panel 3

- Security is not one size; risk based so people can tailor it to their own environment.
- Detection and response need to be prioritized and Incident response plans are key.
- With ransomware, importance of being able to separate back ups from regular systems, because they are actively looking to see if they can get to your backups.

Security Hearing: Panel 4

Panel 4: Federal Perspectives on Security Infrastructure and Enterprise-wide Risk Management in Healthcare

Panelists:

- Julie Chua; HHS Security Risk Management Division Manager, Office of Information Security (OIS) and Government Co-Lead of the 405(d) Task Group
- Timothy Noonan, Deputy Director; Health Information Privacy Division; HHS Office for Civil Rights

Major Themes from Panel 4

- Proactive view of not only enforcement but education
- Revisiting penalty caps - need to catch up with multi-billion-dollar industry
- Cyber should be looked at from all angles not just IT but also Board of Directors, etc.
- Education for C-Suite
- H.R. 7898 (Public Law 116-321), amending HITECH, addresses incentives for cyber
- Focus on small- and medium-need for resources on cybersecurity
- Amplifying existing public-private partnerships and tools

Priorities from Panel 4

- CMPs and CAPs have not been updated for the growth in types of attacks and breadth. It could be an area to explore or develop a position.
- Additional legislation may or may not help.
- We need education and enforcement to compel greater compliance.
- Risk management and risk analysis are seen as vague and cumbersome to do, and that lends itself to not knowing what they are supposed to be assessing.

Relevant Developments

- House Subcommittee on Oversight and Investigations, Committee on Energy and Commerce held a hearing on July 20 – "Stopping Digital Thieves: Growing Threat of Ransomware"
- President Biden signed a National Security Memorandum on "Improving Cybersecurity for Critical Infrastructure Control Systems" which addresses critical infrastructure and implements efforts to meet threats we have.
- White House held a meeting with private sector CEOs to discuss how we can work together to collectively improve the nation's cybersecurity.
- Cyber bill introduced by Sens. Mark Warner, Marco Rubio and Susan Collins that would require private sector companies to work with the government or provide critical infrastructure services to disclose cyberattacks on their system

Recent Federal Updates on Cybersecurity

- Cybersecurity and Infrastructure Security Agency (CISA)
  - Launch of https://www.cisa.gov/stopransomware
  - Release of tips for preventing Ransomware
  - Issuance of blacklist, a catalog of bad practices: https://www.cisa.gov/BadPractices
  - Joint Cyber Defense Collaborative
  - Released August 2021, the Cybersecurity Workforce Training Guide is for current and future federal, state, local, tribal, and territorial (SLTT) staff looking to expand their cybersecurity skills and career options
  - Vulnerability Disclosure Policy (VDP) Platform

- OCR
  - Summer 2021 OCR Cybersecurity Newsletter on Controlling Access to ePHI

Review of Steps from Project Scope

Phase I –Conduct an environmental scan to explore key security challenges and opportunities for securing individually identifiable information in healthcare. The scan will explore existing and emerging frameworks, practices, and technologies to better frame key issues and drivers of change.

Approach: The environmental scan will be accomplished through a virtual hearing and background research to learn from a range of federal agencies, academics, technologists, and thought leaders.

Phase II – Based on what is learned in the environmental scan, develop models and illustrative future scenarios, laying out assumptions, and identifying areas of uncertainty. This is reflective work that the committee will undertake to develop integrative models for how best to secure individually identifiable information and enhance existing enterprise-wide security protections while enabling uses, services, and technology.

Approach: Develop models and identify potential policy, practice, and technology solutions.

Steps from Project Scope, cont.

Phase III - Prepare recommendations for the Secretary of HHS that may include:

- A framework of guiding principles to improve the security posture of the healthcare industry;
- Best practices in security policies and standards across federal agencies and states;
- Levers that HHS can apply such as release of best practices, education, and guidance; and
- Legislative mechanisms, such as enforcement.

Approach: Preparation of a letter for the Secretary.

Steps from Project Scope, cont.

Phase IV – Prepare a report for the health care industry and data stewards and users of health data reflecting a security framework and policy and practice recommendations. This would be modeled on earlier NCVHS stewardship primers and frameworks.

Approach: Report, primer or toolkit

Timeline

	2021 – Q2	2021 – Q 3 & 4	2022 – Q 1 & Q 2	2022 – Q 3
Phase I: Hold a hearing and develop an environmental scan				
Phase II: Develop a draft framework				
Phase III: Prepare and approve a letter to the HHS Secretary				
Phase IV: Prepare a report to the industry.				

Discussion & Questions

- Biggest security opportunities that the health care industry/patient safety should address?

- The most valuable next steps for PCS to focus on?