Annual Report Workgroup

Aaron Miri, Co-Chair
Carolyn Petersen, Co-Chair

November 9, 2018
Agenda

• Call to Order/Roll Call
• Opening Remarks and Workgroup Schedule
• Deeper Dive in Privacy and Security Priority Target Area
  » Presentations
  » Workgroup Discussion
• Planning for Workgroup Update at HITAC Meeting on 11/14/18
• Public Comment
• Next Steps and Adjourn
# Meeting Schedule for Workgroup

<table>
<thead>
<tr>
<th>Month</th>
<th>Deliverables to Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 20, 2018</td>
<td>Workgroup scope for FY18 Annual Report announced</td>
</tr>
<tr>
<td>August 2, 2018</td>
<td>Discuss plans for FY18 Annual Report</td>
</tr>
<tr>
<td>August 24, 2018</td>
<td>Landscape Analysis Outline</td>
</tr>
<tr>
<td></td>
<td>Gap Analysis Outline</td>
</tr>
<tr>
<td>September 20, 2018</td>
<td>Landscape Analysis and Gap Analysis Discussion</td>
</tr>
<tr>
<td>October 18, 2018</td>
<td>Landscape Analysis and Gap Analysis Discussion</td>
</tr>
<tr>
<td></td>
<td>Outline of HITAC Progress in FY18</td>
</tr>
<tr>
<td>November 9, 2018</td>
<td>Privacy and Security Priority Target Area</td>
</tr>
<tr>
<td>December 2018 (TBD)</td>
<td>FY18 Annual Report Draft</td>
</tr>
<tr>
<td>January 10, 2019</td>
<td>FY18 Annual Report Draft</td>
</tr>
<tr>
<td>Winter/Spring 2019</td>
<td>FY18 Annual Report Completed as Needed</td>
</tr>
<tr>
<td>Spring 2019</td>
<td>Work begins on FY19 Annual Report</td>
</tr>
<tr>
<td>Meeting Date</td>
<td>Action Items/Deliverables</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>June 20, 2018</td>
<td>Subcommittee Charge Presented</td>
</tr>
<tr>
<td>September 5, 2018</td>
<td>Workgroup Update</td>
</tr>
<tr>
<td>October 17, 2018</td>
<td>Landscape Analysis and Gap Analysis Update Update</td>
</tr>
<tr>
<td>November 14, 2018</td>
<td>Description of HITAC’s Work in FY18 Reviewed</td>
</tr>
<tr>
<td>January 23, 2019</td>
<td>FY18 Annual Report Reviewed by HITAC</td>
</tr>
<tr>
<td>February 20, 2019</td>
<td>FY18 Annual Report Reviewed/Approved by HITAC</td>
</tr>
<tr>
<td>Winter/Spring 2019</td>
<td>FY18 Annual Report Submitted to HHS Secretary</td>
</tr>
<tr>
<td></td>
<td>FY18 Annual Report Submitted to Congress</td>
</tr>
</tbody>
</table>
Presentations about
Privacy and Security Priority Target Area
"Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges"

Linda Kloss, Chair
Privacy, Confidentiality and Security Subcommittee

November 9, 2018
Outline

1. Highlight findings from NCVHS’s “Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges”

2. Describe the Committee’s “Beyond HIPAA” initiative

3. Suggest how this work might inform ONC’s Annual Report
NCVHS Mandate

• Assist and advise the HHS Secretary on health data, statistics, privacy, national health information policy, and the Department's strategy to best address those issues.

• Assist and advise the Department in the implementation of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA).*

• Inform decision-making about data policy by HHS, states, local governments and the private sector.

  -- NCVHS Charter, approved January 2018

* Reiterated in Section 1104 of the ACA (2010)
1. Identify and describe the changing environment and the risks to privacy and security of confidential health information; highlight promising policies, practices and technology;

2. Lay out integrative models for how best to protect individuals’ privacy and secure health data uses outside of HIPAA protections while enabling useful uses, services and research;

3. Formulate recommendations for the Secretary on actions that HHS and other federal Departments might take; and

4. Prepare a report for health data stewards.
"Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges"

1. Big data and expanding uses and users
2. Personal devices and Internet of Things
3. Laws in other domains (e.g., Fair Credit Reporting restricting uses of consumer data)
4. Evolving technologies for privacy and security
5. Evolving consumer attitude

Key Themes

1. The Regulated (subject to HIPAA) and Unregulated Worlds (not subject to HIPAA).
2. Data in the unregulated category are for the most part, not subject to any specific statutory regulation for privacy.
3. Growing challenge of defining health information, its ownership, control and consent.
4. Selected stories of the world beyond HIPAA illustrating potential risks and harms pertaining to Big data, personal health devices, and the Internet of Things.
5. Opportunity to increase protections and choice for consumers and at the same time reduce burden.
6. Framing legislative issues and approaches such as general data protection.
Beyond HIPAA: Health Information Stewardship Continuum

HIPAA Covered Entities/ Business Associates

All Other Data Users & Data Holders

Compliance Risk >>>> Use & Disclosure Risk

Mechanisms: Public and Private

- Adopt Protections Beyond Regulatory Compliance
- Improve Data Stewardship
- Enact New Data Protections
Applying the Draft Model to Use Cases Operating at the intersection of the HIPAA-covered and unregulated health data world

- **Health Data Registries**: A database storing clinical information collected as a byproduct of patient care existing in various forms and support functions ranging from biomedical informatics, clinical research, public health, epidemiology and evidence based clinical practice.

- **Personal Health Devices** (PHD): A term defined by IEEE to mean a health device which is normally used for measurement by a chronic patient, especially seniors, for telemedicine at home and in other buildings.

- **Geofencing app**: The technology identifies people using cellphones within a certain location and then targets them with ads. In the health space, geofencing is used to market legal services to ED patients and Targeting other messaging to people who visit clinics or other health facilities.

- **Covered Entity**

---


# Use Case: Health Data Registries

<table>
<thead>
<tr>
<th>Leverage current mechanisms</th>
<th>Improve data stewardship</th>
<th>Enact new protections</th>
</tr>
</thead>
</table>
| • Covered entities require data use agreements which include prohibitions against reidentification and redisclosure.  
• Covered entities offer patients opportunity to opt out of registries.  
• CEs strengthen management of de-identified data sets | Voluntary certification of registry sponsors | |

**Private**  
Office for Civil Rights issues guidance for registering Business Associates and Data Use Agreements

**Public**  
Mechanism for accreditation of registries for funding streams  
Registries become covered entities
Beyond HIPAA Progress

- Project Scoping: 2016 & initial Hearings 2017
- Environmental Scan: 2017/18
- Explore "exemplars" at the intersection of regulated and unregulated
- Model Framing: Agreement on approach
  - 13th Report to Congress
- Hearing
- Letter to HHS Secretary
Questions for NCVHS?
NIST Cybersecurity and Privacy Update

Kevin Stine
Chief, Applied Cybersecurity Division
Information Technology Laboratory
National Institute of Standards and Technology
November 9, 2018
Cultivating Trust in Information and Technology Through Cybersecurity And Privacy

Adoption of technologies

Standards

Best practices
We seek to...

- **Equip** organizations to better manage cybersecurity and privacy risk
- **Help** to build a secure infrastructure
- **Energize and promote** a robust ecosystem of cybersecurity education, training, and workforce development
- **Ensure** the right *people* and *things* have the right access to the right resources at the right time
- **Drive** adoption of standards-based cybersecurity
December 18, 2014

Amends the National Institute of Standards and Technology Act (15 U.S.C. 272(c)) to say:

“…on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure”

Cybersecurity Enhancement Act of 2014 (P.L. 113-274)
Key Cybersecurity Framework Attributes
Principles of Current and Future Versions of the Framework

• Common and accessible language
• It’s adaptable to many technologies, lifecycle phases, sectors and uses
• It’s risk-based
• It’s meant to be paired
• It’s a living document
• Guided by many perspectives – private sector, academia, public sector
Cybersecurity Framework Components: Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identify</strong></td>
<td>Asset Management</td>
<td>ID.AM</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
<td>ID.BE</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>ID.GV</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
<td>ID.RA</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
<td>ID.RM</td>
</tr>
<tr>
<td></td>
<td>Supply Chain Risk Management</td>
<td>ID.SC</td>
</tr>
<tr>
<td><strong>Protect</strong></td>
<td>Identity Management and Access Control</td>
<td>PR.AC</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
<td>PR.AT</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
<td>PR.DS</td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes &amp; Procedures</td>
<td>PR.IP</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>PR.MA</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
<td>PR.PT</td>
</tr>
<tr>
<td><strong>Detect</strong></td>
<td>Anomalies and Events</td>
<td>DE.AE</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
<td>DE.CM</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
<td>DE.DP</td>
</tr>
<tr>
<td><strong>Respond</strong></td>
<td>Response Planning</td>
<td>RS.RP</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RS.CO</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
<td>RS.AN</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
<td>RS.MI</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RS.IM</td>
</tr>
<tr>
<td><strong>Recover</strong></td>
<td>Recovery Planning</td>
<td>RC.RP</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
<td>RC.IM</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
<td>RC.CO</td>
</tr>
</tbody>
</table>

**Table:**

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID.BE-1: The organization’s role in the supply chain is identified and communicated</td>
<td>COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A15.1.1, A15.1.2, A15.1.3, A15.2.1, A15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12</td>
</tr>
<tr>
<td>ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated</td>
<td>COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8</td>
</tr>
<tr>
<td>ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated</td>
<td>COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14</td>
</tr>
<tr>
<td>ID.BE-4: Dependencies and critical functions for delivery of critical services are established</td>
<td>COBIT 5 APO10.01, BA104.02, BA109.02 ISO/IEC 27001:2013 A11.2.2, A11.2.3, A12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14</td>
</tr>
<tr>
<td>ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)</td>
<td>COBIT 5 DSS04.02 ISO/IEC 27001:2013 A11.1.4, A17.1.1, A17.1.2, A17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14</td>
</tr>
</tbody>
</table>
Cybersecurity Framework Components: Profile

- Business Objectives
- Threat Environment
- Requirements & Controls

Cybersecurity Profile:
- Identify
- Protect
- Detect
- Respond
- Recover
Cybersecurity Framework Components: Tiers
Supporting Risk Management with the Cybersecurity Framework
Cybersecurity Framework Version 1.1

Risk Management

Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions

Mission Priority and Risk Appetite and Budget

Business/Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget

• Internal
• Supply Chain

Implementation/Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Changes in Current and Future Risk
Implementation Progress
Changes in Assets, Vulnerability and Threat

Implementation

Framework Profiles
Sample Resources

www.nist.gov/cyberframework/industry-resources

Italy’s National Framework for Cybersecurity

American Water Works Association’s
Process Control System Security Guidance for the Water Sector

Financial Services Sector Specific Cybersecurity “Profile”

Sample Resources (Healthcare and Public Health Sector)

www.nist.gov/cyberframework/framework-resources

HHS’s [HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework](https://www.hhs.gov/healthcare/hipaa/index.html)

Symantec’s [Implementing the NIST Cybersecurity Framework in Healthcare](https://www.symantec.com/security-center/reports/nist-cybersecurity-framework)

The Joint HPH Cybersecurity Working Group's [Healthcare Sector Cybersecurity Framework Implementation Guide](https://www.hhs.gov/cybersecurity/)

HITRUST's [Common Security Framework to NIST Cybersecurity Framework mapping](https://www.hitrust.org/)

NIST’s National Cybersecurity Center of Excellence

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs
NIST’s National Cybersecurity Center of Excellence Healthcare Portfolio

**Securing Electronic Health Records on Mobile Devices**
A platform for healthcare providers to securely document, maintain, and exchange electronic patient information among mobile devices.

**Securing Wireless Infusion Pumps**
Helping Healthcare Delivery Organizations secure wireless infusion pumps on an enterprise network.

**Securing Picture Archiving and Communication System**
Providing guidance for securing the PACS ecosystem in healthcare sector organizations.
NIST Cybersecurity Risk Management Conference

Learn about the NIST Cybersecurity Risk Management Conference and register at

Questions & Opportunities to Engage

National Cybersecurity Center of Excellence: https://www.nccoe.nist.gov

Cybersecurity Framework: https://www.nist.gov/cyberframework

Privacy Framework: https://www.nist.gov/privacy-framework

Follow us on Twitter: @NISTcyber

Contact: Kevin Stine, kevin.stine@nist.gov
Questions for NIST?
HHS Office for Civil Rights Cybersecurity Resources

Nicholas P. Heesters, Jr., MEng, JD, CIPP
Health Information Privacy Security Specialist, HHS Office for Civil Rights (OCR)

November 9, 2018
OCR Cybersecurity Resources: Agenda

- HIPAA Security Rule to NIST Cyber Security Framework (CSF) Crosswalk
- HHS Office for Civil Rights Cybersecurity Guidance
- HHS ONC/OCR Security Risk Assessment Tool 3.0
The crosswalk is a response to Executive Order 13636, Improving Critical Infrastructure Cybersecurity, which directed NIST to develop a Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) and to help organizations in various industries understand, communicate, and manage cybersecurity risks. In the health care space, HIPAA covered entities and business associates must comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) that they create, receive, maintain, or transmit.

The crosswalk is not guidance but a voluntary tool to assist organizations in assessing and managing security risks, while also assuring critical operations and service delivery. The crosswalk could also help entities prioritize investments and maximize the impact of each dollar spent on cybersecurity. By mapping the provisions of the different security frameworks, the crosswalk provides a common language that can improve communications, awareness, and understanding about cybersecurity between and among IT, planning, and operating units, as well as senior executives of organizations.
The Office of the National Coordinator for Health Information Technology (ONC) released the crosswalk in February 2016. It was developed in cooperation with the National Institute for Standards and Technology (NIST) and the HHS Office of the National Coordinator for Health Information Technology (ONC).

Organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule may find this crosswalk helpful for identifying potential gaps in their programs. For example, if a covered entity has an existing security program aligned to the HIPAA Security Rule, they can use this mapping document to identify which pieces of the NIST Cybersecurity Framework they are already meeting and which represent new practices to incorporate into its risk management program.
## HIPAA Security Rule to NIST Cybersecurity Framework Crosswalk

<table>
<thead>
<tr>
<th>Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</th>
<th>ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders</th>
</tr>
</thead>
</table>
| ID.RM-2: Organizational risk tolerance is determined and clearly expressed | - COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02
- ISA 62443-2-1:2009 4.3.4.2
- NIST SP 800-53 Rev. 4 PM-9
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B) |
| | - COBIT 5 APO12.06
- ISA 62443-2-1:2009 4.3.2.6.5
- NIST SP 800-53 Rev. 4 PM-9
- HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B) |
The Office of the National Coordinator for Health Information Technology

- Ransomware Guidance
- Cybersecurity Checklist and Infographic
- Cybersecurity Newsletters
  - April 2018: Risk Analysis vs. Gap Analysis
  - May 2018: Workstation Security
  - June 2018: Software Vulnerabilities and Patching
  - July 2018: Guidance on Disposing of Electronic Devices and Media
  - August 2018: Securing Electronic Media and Devices
  - October 2018: National Cybersecurity Awareness Month
The HHS Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR) have updated the popular Security Risk Assessment (SRA) Tool to make it easier to use and apply more broadly to the risks to health information.

The tool is designed for use by small to medium sized health care practices – covered entities, and business associates to help them identify risks and vulnerabilities to ePHI.

The updated tool provides enhanced functionality to document how such organizations can implement or plan to implement appropriate security measures to protect ePHI.


The iOS iPad version was not updated, but the previous version is available at the Apple App Store (search under “HHS SRA Tool”).
SRA Tool New Features and Functionality

- Enhanced User Interface
- Modular Workflow with Question Branching Logic
- Custom Assessment Logic
- Progress Tracker
- Improved Threats & Vulnerabilities Rating
- Detailed Reports
- Business Associate and Asset Tracking
- Overall Improvement of the User Experience
SRA Tool Development Approach

- ONC and OCR conducted comprehensive usability testing of the SRA tool (version 2.0) with health care practice managers.
- Analysis of the findings across the user base informed the development of the content and the requirements for the SRA Tool 3.0.
- ONC and OCR then conducted testing of the SRA tool 3.0 to compare the user experience in completing the same tasks presented in the first round of testing.
- Over the next year, ONC and OCR will continue to gather feedback on the tool to inform future SRA tool modifications and updates. You can give feedback or request help by emailing PrivacyAndSecurity@hhs.gov
SRA Tool Brief Overview of Content

• Section 1: Security Risk Assessment (SRA) Basics (security management process)
• Section 2: Security Policies, Procedures, & Documentation (defining policies & procedures)
• Section 3: Security & Your Workforce (defining/managing access to systems and workforce training)
• Section 4: Security & Your Data (technical security procedures)
• Section 5: Security & Your Practice (physical security procedures)
• Section 6: Security & Your Vendors (business associate agreements and vendor access to PHI)
• Section 7: Contingency Planning (backups and data recovery plans)
The Security Risk Assessment Tool is provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with federal, state or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights Health Information Privacy website.

- Enter your name
- Pick a place to save your SRA
- Name your SRA
- Review the Disclaimer
- Begin your SRA
The SRA tool has 3 core steps:

Step 1: Enter your practice information.
Step 2: Answer the assessment questions.
Step 3: Review your final risk report.

What's a Security Risk Assessment?

A risk assessment is the first step in your Security Rule compliance efforts. Following HIPAA risk assessment guidelines will help you establish the safeguards you need based on the unique circumstances of your health care practice.

- Enter your name
- Pick a place to save your SRA
- Name your SRA
- Review the Disclaimer
- Begin your SRA
• **Practice Information**
  
  » Track Asset Inventory
  
  » Track BAA & Vendors
  
  » Track Documentation
Section 5: Security and the Practice

Select the vulnerabilities that apply to your practice from the list below. Then rate the likelihood and impact on your practice of each potential threat.

- Inadequate procedures for managing facility access where information systems reside
  - Likelihood: Low (L), Medium (M), High (H)
  - Impact: Low (L), Medium (M), High (H)

- Inability to review facility access logs
  - Likelihood: Low (L), Medium (M), High (H)
  - Impact: Low (L), Medium (M), High (H)

- Inability to track and monitor staff/visitors/guests throughout facility
  - Likelihood: Low (L), Medium (M), High (H)
  - Impact: Low (L), Medium (M), High (H)

- Increased response time to respond to facility security incidents
  - Likelihood: Low (L), Medium (M), High (H)
  - Impact: Low (L), Medium (M), High (H)

- Unstructured guidance during facility access decision making
  - Likelihood: Low (L), Medium (M), High (H)
  - Impact: Low (L), Medium (M), High (H)

- Lacks protective measures to prevent physical viewing of ePHI and or sensitive information on computer systems
  - Likelihood: Low (L), Medium (M), High (H)
  - Impact: Low (L), Medium (M), High (H)

- Access granted to unauthorized personnel
  - Likelihood: Low (L), Medium (M), High (H)
  - Impact: Low (L), Medium (M), High (H)

- Disclosure of passwords and or login information
  - Likelihood: Low (L), Medium (M), High (H)
  - Impact: Low (L), Medium (M), High (H)

- The Office of the National Coordinator for Health Information Technology

- Likelihood & Impact Rating
  - Color coded rating system
  - Guided Risk Framework
  - Guidance within ToolTips
Congratulations you’ve completed Section 1, on SRA Basics. Below is a summary highlighting where your practice is meeting the standard and potential areas of improvement.

### Areas of Success

- Q2. Has your practice completed a security risk assessment (SRA) before?
- Q3. Do you review and update your SRA?
- Q4. How often do you review and update your SRA?
- Q5. Do you include all information systems containing, processing, and/or transmitting ePHI in your SRA?
- Q8. Do you respond to the threats and vulnerabilities identified in your SRA?
- Q9. Do you identify specific personnel to respond to and mitigate the threats and vulnerabilities found in your SRA?

### Areas for Review

- Q7. What do you include in your SRA documentation?
- Q10. Do you communicate SRA results to personnel involved in responding to threats or vulnerabilities?

---

**Section Summary**

- **Areas of Success**
- **Areas for Review**
- **Score**
- **Comments & Documents**

**Final SRA Summary**

- **Dashboard**
- **Detailed Report**
Security Risk Assessment Summary

Where is your risk?
Click next for a more detailed report.

37% Risk Score
21 Areas for Review
1 Vulnerabilities

Summary
Dashboard
- Cumulative Risk score
- Risk score by section
- Total Areas for Review
- Total # of Vulnerabilities

Section 1: SRA Basics 22%
Section 2: Security Policies 62%
Section 3: Security & Workforce 16%
Section 4: Security & Data 52%
Questions for OCR?

Nicholas.Heesters@hhs.gov

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
Workgroup Discussion:

Privacy and Security Priority Target Area
Privacy and Security Priority Target Area

• Potential HITAC Activities Identified by Workgroup to Date

  » Opportunity: Increased uniformity of information sharing policies across states. For example, address implications of the California Consumer Privacy Act of 2018.
    – Suggested HITAC Activity: Consider federal role in setting guidelines for exchange of data across states

  » Opportunity: Support for widespread adoption of cybersecurity framework(s)
    – Suggested HITAC Activity: Consider whether a nationwide cybersecurity framework should be adopted
    – Suggested HITAC Activity: Delineate cybersecurity accountability for data by role
Privacy and Security Priority Target Area

• Other Opportunities Identified for Further Consideration

» Education about HIPAA and Confidentiality of Substance Use Disorder Patient Records (a.k.a. 42 CFR Part 2) regulation implications

» Granular levels of consent to share and disclose information

» Address implications of European Union’s General Data Protection Regulation (GDPR) and Privacy Shield

» Education of technology users about privacy and security settings, especially for social media

» Consider what to regulate about the Internet of Things (IoT)

» Continue to improve patient matching when sharing data
Workgroup Discussion:
Update Presentation for HITAC Meeting on 11/14/18
Planning for Update at HITAC Meeting on 11/14/18

• Summarize Workgroup Discussion from Workgroup Meetings on 10/18/18 and 11/9/18:
  » Outline of Section on HITAC Progress in FY18
  » Deeper dive in Privacy and Security Priority Target Area
To make a comment please call:

Dial: 1-877-407-7192

(once connected, press “*1” to speak)

All public comments will be limited to three minutes.

You may enter a comment in the “Public Comment” field below this presentation.

Or, email your public comment to onc-hitac@accelsolutionsllc.com.

Written comments will not be read at this time, but they will be delivered to members of the Workgroup and made part of the Public Record.
Meeting Adjourned

Next Annual Report Workgroup meeting scheduled for 12/6/18, 11:00-12:30 p.m. ET
Additional Slides
## Annual Report Workgroup Membership and ONC Staff

<table>
<thead>
<tr>
<th>Member Name</th>
<th>Organization</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carolyn Petersen</td>
<td>Individual</td>
<td>Co-Chair</td>
</tr>
<tr>
<td>Aaron Miri</td>
<td>The University of Texas at Austin, Dell Medical School and UT Health Austin</td>
<td>Co-Chair</td>
</tr>
<tr>
<td>Christina Caraballo</td>
<td>Audacious Inquiry</td>
<td>HITAC Committee Member</td>
</tr>
<tr>
<td>Brett Oliver</td>
<td>Baptist Health</td>
<td>HITAC Committee Member</td>
</tr>
<tr>
<td>Chesley Richards</td>
<td>Public Health Scientific Services, CDC</td>
<td>Federal Representative</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ONC Staff Name</th>
<th>Title</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Donald Rucker</td>
<td>National Coordinator for Health Information Technology</td>
<td></td>
</tr>
<tr>
<td>Elise Sweeney Anthony</td>
<td>Executive Director, Office of Policy</td>
<td></td>
</tr>
<tr>
<td>Seth Pazinski</td>
<td>Division Director, Strategic Planning &amp; Coordination</td>
<td></td>
</tr>
<tr>
<td>Lauren Richie</td>
<td>Branch Chief, Policy Coordination</td>
<td>Designated Federal Officer (DFO)</td>
</tr>
<tr>
<td>Michelle Murray</td>
<td>Senior Health Policy Analyst</td>
<td>Workgroup ONC Staff Lead</td>
</tr>
</tbody>
</table>
Workgroup Scope

- **Overarching:** The workgroup will inform, contribute to, and review draft and final versions of the HITAC Annual Report to be submitted to the HHS Secretary and Congress each fiscal year. As part of that report, the workgroup will help track ongoing HITAC progress.

- **Detailed:** Provide specific feedback on the content of the report as required by the 21st Century Cures Act including:
  - Analysis of HITAC progress related to the priority target areas
  - Assessment of health IT infrastructure and advancements in the priority target areas
  - Analysis of existing gaps in policies and resources for the priority target areas
  - Ideas for potential HITAC activities to address the identified gaps
HITAC Priority Target Areas: Defined

HITAC Priority Target Areas noted in Section 4003(e) of the 21st Century Cures Act cover the following areas:

- Interoperability – Achieving a health information technology infrastructure that allows for the electronic access, exchange, and use of health information
- Privacy and Security – The promotion and protection of privacy and security of health information in health IT
- Patient Access – The facilitation of secure access by an individual and their caregiver(s) to such individual’s protected health information
- Any other target area related to the above target areas that the HITAC identifies as an appropriate target area to be considered on a temporary basis with adequate notice to Congress