OSCAL Workshop: Applicability of OSCAL for Healthcare

March 2nd, 2022
Our Presenter

Vikas Khosla
Chief Digital Health Security Officer

- 20+ years in Healthcare Security, Privacy and Compliance
- Previously founded and lead 100% healthcare security consultancy
- Focused on optimization of enterprise security programs
- Host of “Virtual Coffee Chats with Vikas” podcast
• Current Landscape and Regulations in Healthcare

• Special Challenges in the Healthcare Sector

• The Need for Scalability and Standards

• Sample of OSCAL Automation

• OSCAL APIs: Achieving a “Single Pane of Glass View of Risks”

• Q&A
# Healthcare Sector Feeling “Cybersecurity-Pressure”

<table>
<thead>
<tr>
<th><strong>34%</strong></th>
<th>Share of global healthcare sector suffering a ransomware attack in the last year</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>33%</strong></td>
<td>Percentage of all third-party breaches targeting healthcare</td>
</tr>
<tr>
<td><strong>45,000,000</strong></td>
<td>Number of healthcare records stolen or exposed in 2021</td>
</tr>
<tr>
<td><strong>$250</strong></td>
<td>Value of a Healthcare Record</td>
</tr>
<tr>
<td><strong>$5</strong></td>
<td>Value of Credit Card data</td>
</tr>
<tr>
<td><strong>8M hours - $2B annually</strong></td>
<td>Healthcare industry level of effort and cost to perform a manual HIPAA Security Assessment</td>
</tr>
</tbody>
</table>

*Includes physician practices, hospitals and health insurers

(Source: [Intraprise Health](#))
Stark Safe Harbor

- Allows for the donation of cybersecurity technology (including hardware) and related services if certain conditions are met.

HIPAA Privacy Rule Proposed Changes

- Better support individuals’ engagement in their care, remove barriers to coordinated care, and reduce regulatory burdens on the healthcare industry

HIPAA/HITECH Safe Harbor (H.R. 7898)

- When investigating/undertaking HIPAA enforcement the legislation directs HHS to consider the use of industry-standard security practices, cybersecurity preparedness when calculating fines, and decreased audit lengths.
Industry-wide Challenges

**Time Consuming**
- What type of assessment? Security, Privacy, Both?
- Hundreds of different vendors providing services
- PHI & PII compliance requirements (HIPAA, PCI)

**Manual Process**
- Entire process is managed via spreadsheets, Word docs and email
- Many emails back and forth with vendors
- Difficult to keep track of past/present/future assessments

**Few Resources**
- Often one or two employees managing all assessments
- Extremely difficult to manage all assessments and communication with a small team
- Full-time job to manage entire program

**Accelerate Assessments**
- Major health crisis (COVID-19)
- Need to accelerate assessments of new solutions/innovations
- No time for delays! Patience-care and safety on the line
OSCAL sets the foundation for automation and interoperability

OSCAL enables tools and organizations to exchange risk information via automation

- Service Providers
- Third Party Apps & Hardware
- Research Partners
- Patient Care
- HIPAA
- Health IT Systems
- Medical Device IoT

"The Rosetta Stone" for Healthcare Assessors
Building a Centralized Repository of Compliance Standards and Risk Data using OSCAL

• Utilize Standards to accelerate Compliance and Cyber-Resilience
• “Single-Pane of Glass” View of Risks – Unified, Normalized and Interoperable
• Scalable across healthcare sector participants
• Significant overlap of companies doing business with federal and healthcare sector customers
Before: Manual Third-Party Assessment Process

New Contract
New Product
New Service
New Vendor

Assessor

Report

Security Committee

Approve
Deny

Third Party
After: Automated Third-Party Assessment Process

- Internal Personnel → Submit Assessment Request
- Third Party → Provide Information
- IH Assessor → Conduct Assessment

Report

Security Committee
- Approve
- Deny

Status Tracking
OSCAL and RMF enabled Integrated Risk Management

Single Pane of Glass View of Risks
Built on NIST RMF 2.0 and OSCAL

- Internal and External HIPAA Assessments
- Third-Party/Vendor Risk Management
- Policies and Procedures
- Breach Notification & Vulnerability Sources
- Network/Threat Mgmt Sources
- Med IoT Risks and Vulnerabilities
- OSCAL API Layer

Compliance, Financial and Business Risks

HIPAA and NIST Security and Privacy Risk Assessments
TPRM Assessments
Portfolio Manager
Plan-of-Action Manager
Enterprise Risk Register, Dashboards and Analytics

© 2022 All Rights Reserved.
Informed Decision Making

- Enterprise, Holistic View
- Drive Program Maturity
- Assessment and Workflow Automation
- Analytics and Visualizations

IRM Dashboards
TPRM Dashboards