EHEALTH COMMISSION MEETING

JULY 11, 2018
<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00</td>
<td>Call to Order</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Roll Call and Introductions, Approval of April, May and June Minutes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>July Agenda and Objectives</td>
<td></td>
</tr>
<tr>
<td>12:05</td>
<td>Announcements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OeHI Updates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>State Agency, Community Partner, and SIM HIT Updates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Opportunities and Workgroup Updates</td>
<td></td>
</tr>
<tr>
<td>12:10</td>
<td>Information Security- Part 1: NIST, GDPR</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>David Ginsberg, President, PrivaPlan Associates Inc.</em></td>
<td></td>
</tr>
<tr>
<td>12:15</td>
<td>Information Security-Part 2: HITRUST Organizational Readiness</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Trent Hein, Co-Founder and Former CEO, AppliedTrust</em></td>
<td></td>
</tr>
<tr>
<td>12:25</td>
<td>Discussion/Initiative: Cybersecurity Operational Best Practices</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Mary Anne Leach, Director, OeHI</em></td>
<td></td>
</tr>
<tr>
<td>12:35</td>
<td>Health IT Roadmap- Six (6) Month Progress Report</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Mary Anne Leach, Director, Office of eHealth Innovation</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Carrie Paykoc, State Health IT Coordinator</em></td>
<td></td>
</tr>
<tr>
<td>1:30</td>
<td>Public Comment Period</td>
<td></td>
</tr>
<tr>
<td>1:45</td>
<td>Closing Remarks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Open Discussion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recap Action Items</td>
<td></td>
</tr>
<tr>
<td></td>
<td>August Agenda</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adjourn</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adjourn</td>
<td></td>
</tr>
<tr>
<td>1:55</td>
<td>Michelle Mills, Co-Chair</td>
<td></td>
</tr>
</tbody>
</table>
OeHI UPDATES

- New Intern, Jessica Yan
- **OeHI Connects**: 2nd Quarter Newsletter
- Colorado Health IT Roadmap: 6 Month Progress Report
- **HB18-1198**: Boards and Commissions update, best practices
- Prime Health & Critical Access Hospitals
- OeHI Operating Budget Request for FY19/20
- Formulating policy proposals for next legislative session

COMMISSION UPDATES
<table>
<thead>
<tr>
<th>Action Item</th>
<th>Owner</th>
<th>Timeframe</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update quorum bylaws</td>
<td>OeHI Director</td>
<td>Feb 2018</td>
<td>In progress</td>
</tr>
<tr>
<td>Track and report federal and local legislation</td>
<td>OeHI Director / State Health IT Coordinator</td>
<td>2018</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Letter to Lab Corps and Quest</td>
<td>OeHI Director / Govs Office / Morgan</td>
<td>2017</td>
<td>In progress</td>
</tr>
<tr>
<td>Roadmap Communication Packet</td>
<td>OeHI Director / State Health IT Coordinator</td>
<td>Feb 2018</td>
<td>-Templates available</td>
</tr>
</tbody>
</table>
INFORMATION SECURITY

HITRUST

NIST

DAVID GINSBERG, PRESIDENT, PRIVAPLAN ASSOCIATES INC.
COLORADO EHEALTH COMMISSION
JULY 11, 2018
Topics today

- U.S. Regulatory environment for cybersecurity
- European Union-GDPR
- Other nations? - Canada, South America
- U.S. Standard setting - NIST
- Colorado health care and cybersecurity - a report card
U.S. Regulatory environment

- HIPAA

- State regulations protecting personal information

- These are undergoing upgrades-for example Colorado HB18-1128:
  - Affects all CO businesses and extends the HIPAA definition of covered entity
  - Expands PHI data elements to include a new data combination-email/user name with a password or security question!
General Data Protection Regulation

- Builds upon previous regulations and enhances the use of old definitions and new definitions:
  - Data subject="subject individual" in HIPAA
  - “Right to be forgotten”=data erasure
  - Data Protection Officer=Privacy or Security Official in HIPAA
  - Data Controller=Covered entities like hospitals/providers
  - Opt-In Consent vs Opt Out (ie CORHIO)
  - Psuedonymization=data masking=de-identification
European Union

GDPR introduces the concept of privacy by design

Interestingly, a closer read of the ONC Certified EHR Technology for Stage 3 or 2015 Edition leads to a similar conclusion as best practice for building data security into EHR systems
European Union

Does GDPR apply to Colorado organizations?
Other Nations?

- Canada has had laws in place since 2004

- Central and South America—and these are evolving:
  - Suriname is introducing new law
  - Chile adopted a revised regulation in April
National Institute of Standards and Technology

• Maintains a laboratory environment for various technology standards
• Over past decade has published numerous “Special Publications” on information security
• NIST has also worked with the Office of the National Coordinator and HHS/OCR to provide alignment to the HIPAA security rule-and in some cases specific reference to standards.
• For example, NIST’s definitions for data being rendered unreadable, unusable or indecipherable
NIST SP 800-53

Security and Privacy Controls for Organizations

• Now in draft form for Revision 5
• Final Public Draft in October
• Major upgrade from Rev 4 recognizing the enmeshment of privacy with data security
• Promotes privacy by design concepts
• Next generation of controls for authentication recognizing that passwords may be less critical in an era of multifactor authentication/identity management
• Will remain the standard for setting security controls

Copyright PrivaPlan® Associates, Inc. 2018
NIST Cyber Security Framework

A new framework to apply controls

• Classifies the framework or set of controls and safeguards
• ONC refers to this in its guidance for HealthIT
• We have applied this as an overlay to a HIPAA security risk analysis for health providers and business associates
As a result of:

- Continuous risk analyses for Colorado Rural Health Center members (33 rural hospitals and numerous clinics)
- A series of COPIC compliance wellness “checks” in 2017
- Numerous other Colorado covered entities like National Jewish, Primary Care Partners

PRIORITIES:

- Business Associate management
- Data classification-unknown applications and risks
- Termination management
- True Intrusion Detection
- Social engineering
Wrap Up

David Ginsberg
303-883-7760
dginsberg@privaplan.com
PRIORITIES IN EHEALTH CYBERSECURITY

Trent R. Hein, CISSP, CCIE, ISSMP, ISSAP, PCI QSA, CSSA
trent@rule4.com
HOW WE GOT HERE

Increasing dependence on technology increases cybersecurity risk.
WHAT ARE WE TRYING TO PROTECT?

1. Availability
2. Information Security
3. Integrity
4. Confidentiality
WHY?

- Cost?
- Compliance?
- Public image?
- “Right thing to do”?
- News reports / media coverage sounded scary?
- Protect ability to provide patient care?
- Everybody else is doing it?
# PER-RECORD COST OF BREACH

<table>
<thead>
<tr>
<th>Industry</th>
<th>Average Cost Per Record Breached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>$355</td>
</tr>
<tr>
<td>Education</td>
<td>$246</td>
</tr>
<tr>
<td>Financial</td>
<td>$221</td>
</tr>
<tr>
<td>Services</td>
<td>$208</td>
</tr>
<tr>
<td>Life science</td>
<td>$195</td>
</tr>
<tr>
<td>Retail</td>
<td>$172</td>
</tr>
<tr>
<td>Communications</td>
<td>$164</td>
</tr>
<tr>
<td>Industrial</td>
<td>$156</td>
</tr>
<tr>
<td>Energy</td>
<td>$148</td>
</tr>
<tr>
<td>Technology</td>
<td>$145</td>
</tr>
<tr>
<td>Hospitality</td>
<td>$139</td>
</tr>
<tr>
<td>Consumer</td>
<td>$133</td>
</tr>
<tr>
<td>Media</td>
<td>$131</td>
</tr>
<tr>
<td>Transportation</td>
<td>$129</td>
</tr>
<tr>
<td>Research</td>
<td>$112</td>
</tr>
<tr>
<td>Public</td>
<td>$80</td>
</tr>
</tbody>
</table>

*Healthcare and finance experienced larger costs*  
*Currencies converted to US dollars*
THERE IS NO ZERO-RISK POSITION

No one approach, product, vendor, consultant, amazing CISO, ceremonial dance, sanction, or directive makes this problem disappear.
LIKELIHOOD AND IMPACT

- Certain
- Likely
- Unlikely
- Impossible
SPOT THE OPPORTUNITIES
SPOT THE OPPORTUNITIES
CHALLENGES

▪ Users
  ▪ Awareness
  ▪ Behavior
  ▪ Culture
  ▪ Modeling by leadership

▪ Biomed/IoMT
  ▪ Awareness
  ▪ Who owns it?
  ▪ Vendor management

▪ Proactive prioritization and funding of cybersecurity
## STANDARDS

<table>
<thead>
<tr>
<th>General</th>
<th>Domain specific</th>
<th>Converged</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001/27002</td>
<td>HIPAA</td>
<td>HITRUST</td>
</tr>
<tr>
<td>NIST 800-series (800-30, 800-53, 800-171, CSF, etc.)</td>
<td>PCI DSS</td>
<td></td>
</tr>
<tr>
<td>Common Criteria</td>
<td>NERC CIP</td>
<td></td>
</tr>
<tr>
<td>COBIT</td>
<td>Privacy: GDPR, US state regs, etc.</td>
<td></td>
</tr>
</tbody>
</table>
STANDARDS

- **Benefits**
  - Comprehensive / “What did I forget?”
  - Communicate to external parties your security profile
  - Ready-made roadmap
  - Be like the cool kids

- **Challenges**
  - Checkbox mentality
  - Not adapted to YOUR organization
  - Reaching the goal doesn’t mean you’re secure
HITRUST

- Non-profit alliance formed in 2007 consisting of many interested parties (providers, vendors, etc.)
- Exists to ensure information security becomes a core pillar of, rather than an obstacle to, broad adoption of health information systems and exchanges
- Rationalizes regulations and standards into a single overarching framework tailored for the healthcare industry
- HITRUST standard itself is “free” to healthcare providers, but actual 3rd party certification involves both the provider and the 3rd party paying significant fees to HITRUST alliance
HITRUST CSF

- Includes, harmonizes and cross-references existing, globally recognized standards, regulations and business requirements, including ISO, NIST, PCI, HIPAA, and EU and State laws
- Scales controls according to type, size and complexity of an organization
- Provides prescriptive requirements to ensure clarity
- Follows a risk-based approach offering multiple levels of implementation requirements determined by specific risk thresholds
- Allows for the adoption of alternate controls when necessary
- Evolves according to user input and changing conditions in the industry and regulatory environment on an annual basis
- Provides an industry-wide approach for managing Business Associate compliance
# CSF DOMAINS

<table>
<thead>
<tr>
<th>CSF Assessment Domains</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Protection Program</td>
<td>Data Protection and Privacy</td>
</tr>
<tr>
<td>Mobile Device Security</td>
<td>Risk Management</td>
</tr>
<tr>
<td>Endpoint Protection</td>
<td>Third Party Security</td>
</tr>
<tr>
<td>Wireless Protection</td>
<td>Access Control</td>
</tr>
<tr>
<td>Portable Media Security</td>
<td>Incident Management</td>
</tr>
<tr>
<td>Password Management</td>
<td>Education, Training, and Awareness</td>
</tr>
<tr>
<td>Transmission Management</td>
<td>Assessment Logging and Monitoring</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Business Continuity and Data</td>
</tr>
<tr>
<td>Network Protection</td>
<td>Recovery</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>Physical and Environmental Security</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
PATH TO HITRUST

▪ Self-Assessment
  ▪ No validation
  ▪ 3rd party can facilitate, provide feedback

▪ CSF Assessor Validated
  ▪ HITRUST approved CSF Assessor
  ▪ Interviews
  ▪ Technical testing
HITRUST RECOMMENDATIONS

- HITRUST is huge - not a good “starter standard.” Tackle HITRUST only after you’ve tried something else (NIST, ..)
- May not be best fit for small orgs / providers
- Always ask WHY. What is the business or patient benefit of pursuing HITRUST?
- Culture and leadership is essential in implementing ANY standard
PRACTICAL STEPS TO SECURITY

1. Know the WHY - Why does cybersecurity matter to your organization?

2. Have a plan
   - Decide on a framework (NIST, HITRUST, ISO, whatever)
   - Prioritize efforts based on risk

3. Know your environment - Where is the data and risk?
   - Understand your business and organization
   - What are you trying to protect?
   - Where is it stored / handled? Don’t forget about IoMT devices.

4. Establish a culture of awareness and secure behaviors for all users and especially leadership
CYBERSECURITY DISASTER PREPAREDNESS

▪ You must have a cybersecurity incident response plan
  ▪ ... and you don’t really have one unless you perform regular live drills
  ▪ ... like every few months
  ▪ ... for real, I’m not kidding

Like so many things, know the WHY for incident response.
▪ Patient care and life safety should be job #1
▪ Again, don’t forget about Biomed/IoMT

▪ Every organization (large, small, regardless of security maturity) should join an ISAC
  ▪ National Healthcare ISAC - https://nhisac.org/
QUESTIONS?
THANK YOU!

Trent R. Hein
trent@rule4.com
ROADMAP INITIATIVE #9
PROMOTE CYBERSECURITY
BEST PRACTICES

MARY ANNE LEACH, DIRECTOR, OEHI
COLORADO HEALTH IT ROADMAP

SIX (6) MONTH PROGRESS REPORT

MARY ANNE LEACH, DIRECTOR, OEHI
CARRIE PAYKOC, STATE HIT COORDINATOR, OEHI
SIX (6) MONTH PROGRESS REPORT

- Roadmap Communications
  - Emailed and distributed over 350 copies

- Roadmap Funding
  - State 10% funding secured
  - CMS 90% funding - IAPD submitted, expected by September
  - OeHI Operating Budget for State FY 19/20 submitted
  - $40M in capital and operating funds through Sept. 2021

- Roadmap Governance
  - HIE & Data Sharing Work Group
  - Care Coordination Work Group
  - Consumer Engagement Work Group (forming)
SIX (6) MONTH PROGRESS REPORT

- **Roadmap Initiative #1: Care Coordination**
  - Survey, interviews conducted
  - Several possible opportunities identified

- **Roadmap Initiative #2: Consumer Engagement / Empowerment**
  - 9News and OeHI consumer survey conducted
  - Starting August: Plan to conduct interviews, focus groups statewide; identify objectives, resources and gaps, requirements

- **Roadmap Initiative #3: Advance HIE & Data Sharing**
  - Both HIEs pursuing Social Determinants of Health; data integration
  - PDMP integration achieved with both HIEs
  - State Agency Data Sharing Agreement, State HIT WG
  - County Data Sharing Efforts
  - Colorado Evaluation and Action Lab (COLAB)
Roadmap Initiative #6: Health IT PMO
- Hired first Program Manager for EHR/HIE programs
- Held discussions with HTS and with OIT re: approach

Roadmap Initiative #11: Digital Health Innovation
- Prime Health Summit & 10.10.10
- Focusing on several roadmap initiatives
- Connecting and aligning individual innovators, resources

Roadmap Initiative #13: Ease Quality Reporting Burden
- Contracted and started work with SIM on eCQMs with CORHIO, QHN, CCMCN
Roadmap Initiative #14: Unique Person Identification

- Developed MPI, MPD, and MDM requirements
- MPI RFI issued, and Public Comments integrated
- SIDMOD (Medicaid number/identifier) - current state analysis and replacement requirements are nearing completion
- Evaluation of CORHIO / Verato (5.4M individuals) underway

Roadmap Initiative #15: Unique Provider Identification

- Progress continues at CDPHE

Roadmap Initiative #16: Broadband and Virtual Care

- Office of Broadband: April, 2018, Governor Hickenlooper signs bill for $100M in funding for rural, underserved areas in Colorado
CLOSING REMARKS, AUGUST AGENDA, AND ADJOURN

MICHELLE MILLS, CO-CHAIR
Call to Order
   Roll Call and Introductions, Approval of July Minutes, August Agenda and Objectives  12:00

Announcements  12:10
   OeHI Updates
   State Agency and SIM HIT Updates
   Grant Opportunities, Workgroup Updates, Announcements

New Business

   Prevention Alliance

   Mosiaca Partners: Consumer Engagement & Empowerment  1:05

   Other topics?  1:30

Remaining Commission Comments  1:45
Public Comment Period  1:50
Closing Remarks  1:55
   Open Discussion, September Agenda, Adjourn