OeHI
Office of eHealth Innovation

EHEALTH COMMISSION MEETING

JULY 11, 2018

JULY AGENDA

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

ANNOUNCEMENTS

OeHI Office of eHealth Innovation

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

ACTION ITEMS

Action Item	Owner	Timeframe	Status
Update quorum bylaws	OeHI Director	Feb 2018	In progress
Track and report federal and local legislation	OeHI Director/ State Health IT Coordinator	2018	Ongoing
Letter to Lab Corps and Quest	OeHI Director/ Govs Office/ Morgan	2017	In progress
Roadmap Communication Packet	OeHI Director/ State Health IT Coordinator	Feb 2018	-Templates available

OeHI
Office of eHealth Innovation

INFORMATION SECURITY

HITRUST
NIST

DAVID GINSBERG, PRESIDENT, PRIVAPLAN ASSOCIATES INC.

COLORADO EHEALTH COMMISSION
JULY 11, 2018

2018

PRESENTED BY: DAVID A. GINSBERG, PRESIDENT, PRIVAPLAN ASSOCIATES, INC

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!

European Union

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

NIST

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

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

CO Report Card

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

OeHI
Office of eHealth Innovation

PRIORITIES IN EHEALTH CYBERSECURITY

Trent R. Hein, CISSP, CCIE, ISSMP, ISSAP, PCI QSA, CSSA

trent@rule4.com

OeHI
Office of eHealth Innovation

HOW WE GOT HERE

Increasing dependence on technology increases cybersecurity risk.

OeHI
Office of eHealth Innovation

WHAT ARE WE TRYING TO PROTECT?

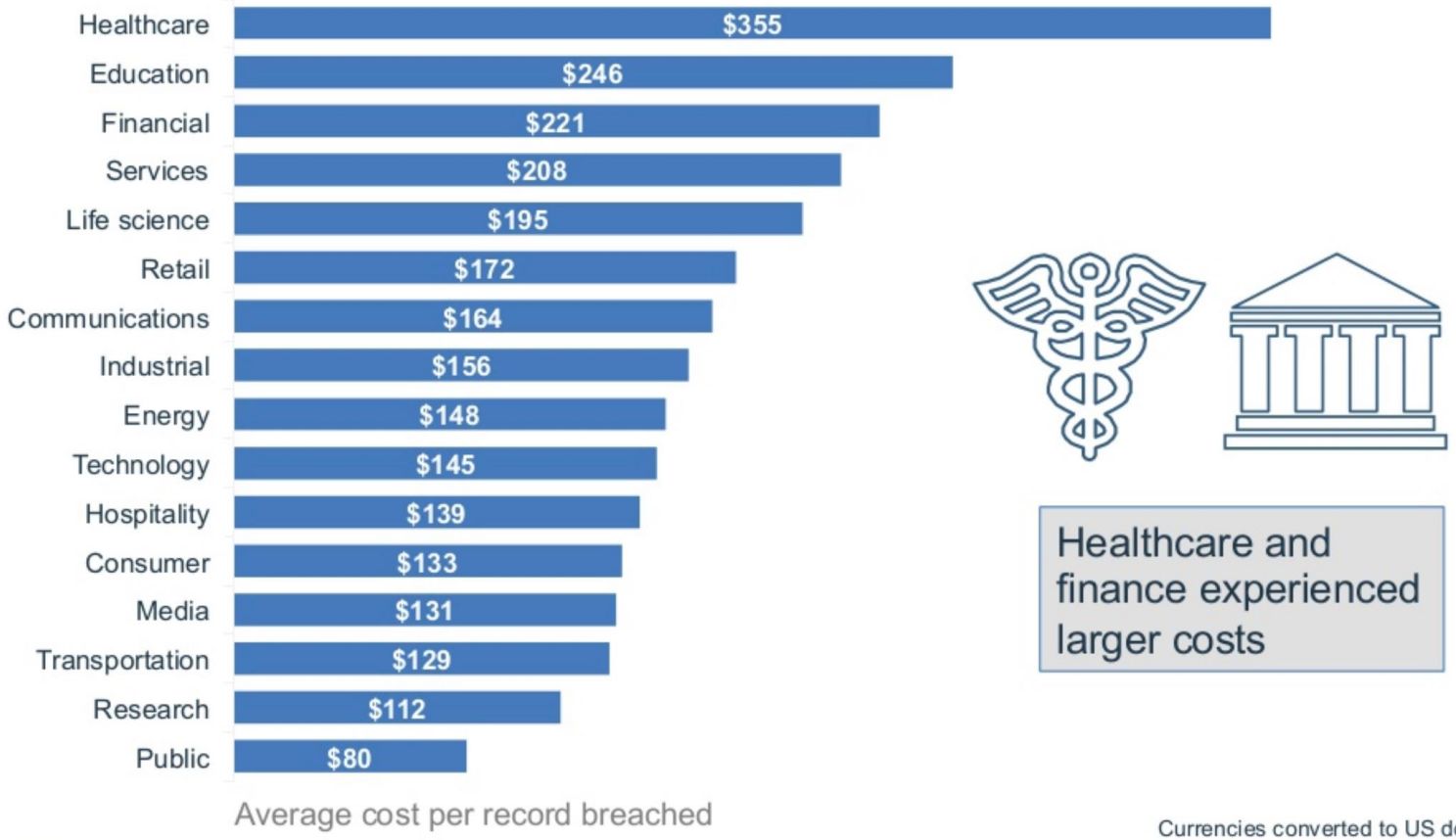
OeHI
Office of eHealth Innovation

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?

OeHI
Office of eHealth Innovation

PER-RECORD COST OF BREACH



THERE IS NO ZERO-RISK POSITION

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

OeHI
Office of eHealth Innovation

LIKELIHOOD AND IMPACT

Certain

Likely

Unlikely

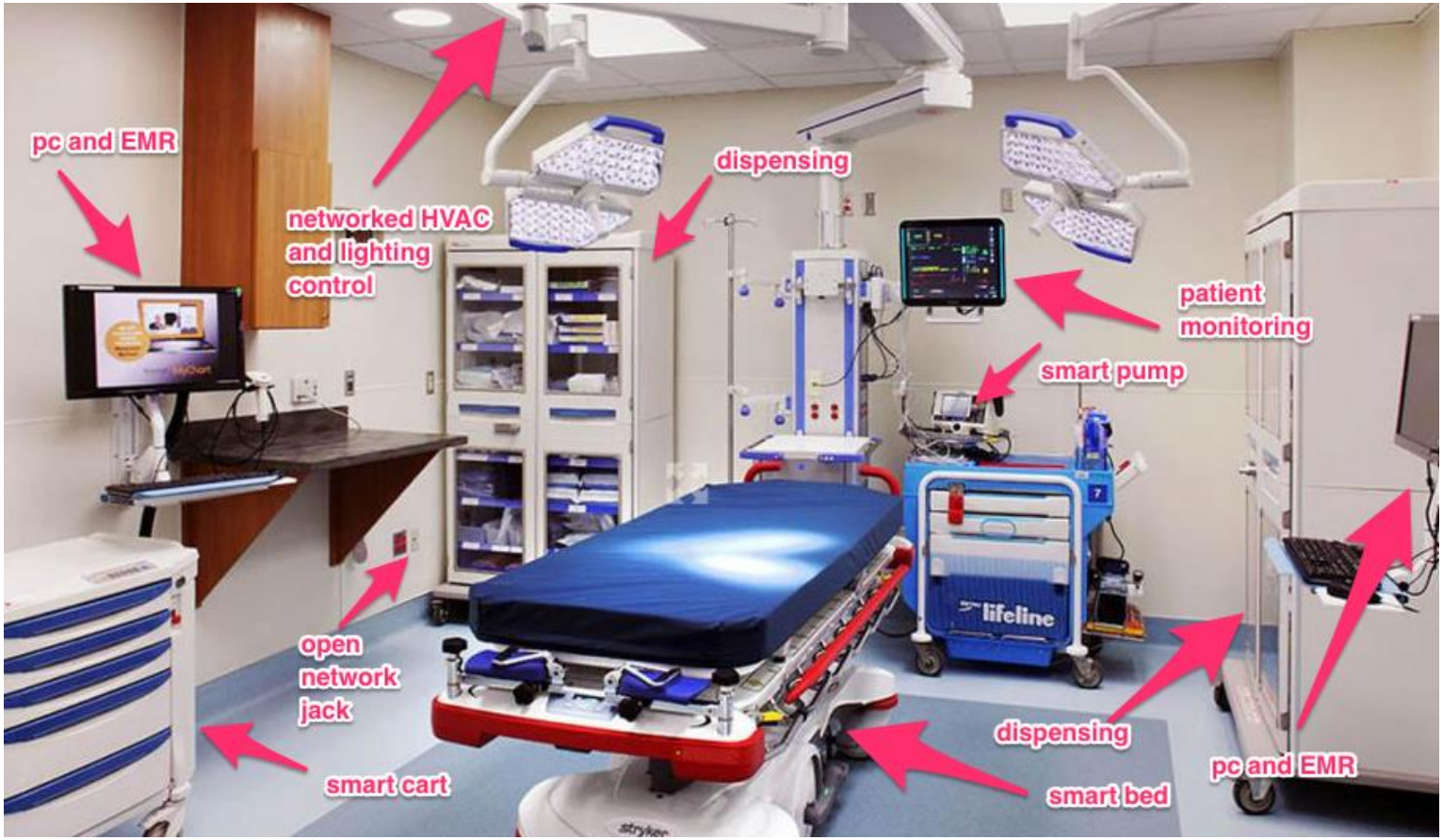
Impossible

OeHI
Office of eHealth Innovation

SPOT THE OPPORTUNITIES

OeHI
Office of eHealth Innovation

SPOT THE OPPORTUNITIES



OeHI
Office of eHealth Innovation

CHALLENGES

- Users
  - Awareness
  - Behavior
  - Culture
  - Modeling by leadership
- Biomed/IoMT
  - Awareness
  - Who owns it?
  - Vendor management
- Proactive prioritization and funding of cybersecurity

STANDARDS

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

OeHI
Office of eHealth Innovation

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

OeHI
Office of eHealth Innovation

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

OeHI
Office of eHealth Innovation

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

OeHI
Office of eHealth Innovation

CSF DOMAINS

CSF Assessment Domains	
Information Protection Program	Data Protection and Privacy
Mobile Device Security	Risk Management
Endpoint Protection	Third Party Security
Wireless Protection	Access Control
Portable Media Security	Incident Management
Password Management	Education, Training, and Awareness
Transmission Management	Assessment Logging and Monitoring
Configuration Management	Business Continuity and Data Recovery
Network Protection	Physical and Environmental Security
Vulnerability Management	

OeHI
Office of eHealth Innovation

PATH TO HITRUST

- Self-Assessment
  - No validation
  - 3rd party can facilitate, provide feedback
- CSF Assessor Validated
  - HITRUST approved CSF Assessor
  - Interviews
  - Technical testing

OeHI
Office of eHealth Innovation

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

OeHI
Office of eHealth Innovation

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/

OeHI
Office of eHealth Innovation

QUESTIONS?

OeHI
Office of eHealth Innovation

THANK YOU!

Trent R. Hein
trent@rule4.com

OeHI
Office of eHealth Innovation

ROADMAP INITIATIVE #9
PROMOTE CYBERSECURITY BEST PRACTICES

MARY ANNE LEACH, DIRECTOR, OEHI

OeHI
Office of eHealth Innovation

COLORADO HEALTH IT ROADMAP

SIX (6) MONTH PROGRESS REPORT

MARY ANNE LEACH, DIRECTOR, OEHI
CARRIE PAYKOC, STATE HIT COORDINATOR, OEHI

OeHI
Office of eHealth Innovation

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)

OeHI
Office of eHealth Innovation

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)

OeHI
Office of eHealth Innovation

SIX (6) MONTH PROGRESS REPORT

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

SIX (6) MONTH PROGRESS REPORT

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

OeHI
Office of eHealth Innovation

CLOSING REMARKS, AUGUST AGENDA, AND ADJOURN

MICHELLE MILLS, CO-CHAIR

DRAFT AUGUST AGENDA

OeHI
Office of eHealth Innovation

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 Open Discussion, September Agenda, Adjourn	1:55