
HIT/HIE Community and Organizational Panel

Office of
Health Information Technology

January 14, 2016

The logo for the Oregon Health Authority. It features the word "Oregon" in a smaller, orange, serif font positioned above the "H" of the word "Health". The word "Health" is in a large, dark blue, serif font. Below "Health", the word "Authority" is written in a smaller, orange, serif font. A thin blue horizontal line is positioned just above the "Authority" text, extending from the left side of the "H" in "Health" to the right edge of the "Authority" text.

Oregon
Health
Authority

Welcome, Introductions, and Agenda Review



Agenda

- OHA Behavioral Health Information Sharing Advisory Group: Update and discussion
- Jefferson HIE ONC Grant: Update and discussion
- HealthTech Solutions: Security Lifecycle presentation and discussion
- HITOC Charter, workplan and priorities
- Roundtable: Brief updates, successes, and challenges
- HCOP future topics

Behavioral Health Information Sharing Advisory Group

Veronica Guerra, Policy Lead

Melissa Isavoran, Policy Lead



Agenda Goals

- Review of the Behavioral Health Information Sharing Workgroup
- Advisory Group work plan and timeline
- Overview of webinars
- Next steps and resources

Overview of the Advisory Group

- **Need:** Lack of understanding of Part 2 and state laws impacted CCOs' care coordination ability
- **Goal:** To develop solutions to support integrated care and enable sharing of behavioral health information between behavioral and physical health providers
- **Members/Partners:** Internal staff from across the agency

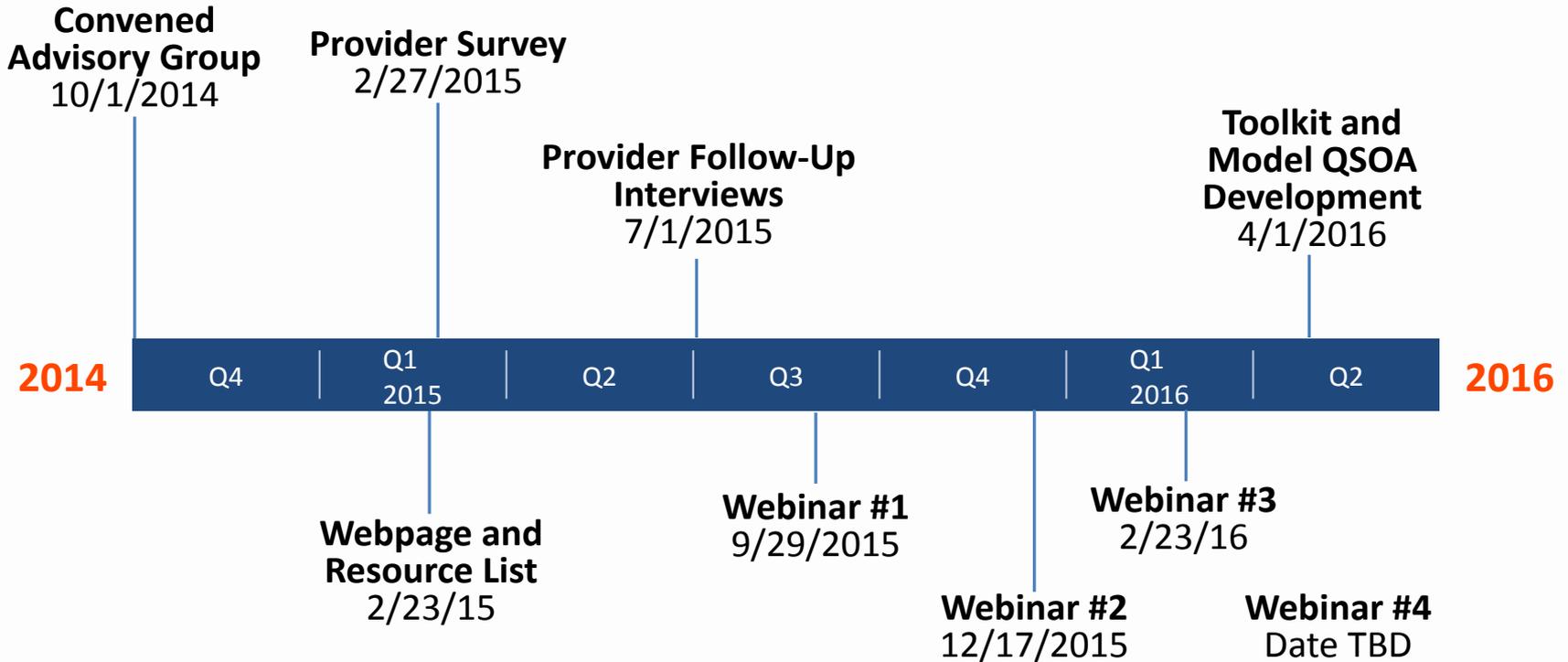
Priorities:

- Outreach to stakeholders
- Education
- Leverage existing IT solutions
- Develop tools to facilitate information sharing

Advisory Group Work Plan

- Conduct provider survey to understand barriers to sharing behavioral health information
- Develop a webpage with resources for providers
- Conduct a series of webinars
- Develop a model Qualified Service Organization Agreement (QSOA) for use with Part 2 providers and HIEs
- Develop a toolkit covering privacy laws, case studies of allowable sharing, model forms (consent and QSOA), and FAQs
- Engage federal partners in discussions about modifications to Part 2

Timeline



Webinars

- **Webinar #1: September 29, 2015**
 - Topic: Overview of state and federal privacy laws
 - Presenters: SAMSHA, the Legal Action Center, and the Oregon Department of Justice
 - Attendees: 300
- **Webinar #2: December 17, 2015**
 - Topic: Deeper dive into federal privacy laws with use case examples from providers
 - Presenters: Robert Belfort, from Manatt, Phelps & Phillips, LLP
 - Attendees: 275
- **Webinar #3: February 2016**
 - Topic: Overview of Oregon's HIT/HIE infrastructure and current work on behavioral health information sharing
 - Presenters: Susan Otter, OHA Office of Health Information Technology, and Gina Bianco, Jefferson HIE
- **Webinar #4: April/May 2016**
 - Topic: Overview of provider toolkit on behavioral health information sharing and intended uses.

OHA's Next Steps

- Legal Action Center Actionline services
- Conduct two additional webinars
- Develop a model Qualified Service Organization Agreement
- Collaborate on OHA and Jefferson HIE ONC grant
- Develop a provider toolkit covering privacy laws, case studies of allowable sharing, model forms, and FAQs
- Engage federal partners in discussions about modifications to Part 2
- Continue to consult with other states

Resources

For more information about the Behavioral Health Information Sharing Advisory Group and access to webinar recordings, please visit:

<http://www.oregon.gov/oha/amh/Pages/bh-information.aspx>



JEFFERSON
HEALTH
INFORMATION
EXCHANGE

ONC Advanced HIE Cooperative Agreement Project Update

HIT/HIE Community and
Organizational Panel Meeting

January 14, 2014

Gina E. Bianco, MPA
Acting Director

Grant Funded Projects

- ▶ New Data Sources
 - Discrete hospital data & ambulatory CCD
- ▶ Sequoia Project Certification
 - VA Data Exchange
- ▶ Clinical Event Notifications
 - Integrated with Community Health Record
- ▶ PDMP Connectivity
 - Dependent upon legislative change
- ▶ Behavioral Health Information Exchange



JEFFERSON
HEALTH
INFORMATION
EXCHANGE

BH Project Approach

- ▶ Develop universal interpretation of law for the exchange, disclosure, and re-disclosure of drug, alcohol and mental health data
- ▶ Develop common consent management model (CMM)
 - Common Release of Information form
 - Requirements for electronic data exchange
- ▶ Implement CMM within JHIE technology to enable robust exchange
- ▶ Connect with behavioral health EHRs



JEFFERSON
HEALTH
INFORMATION
EXCHANGE



JEFFERSON
HEALTH
INFORMATION
EXCHANGE

Behavioral Health Data Exchange Legal Findings

Managing Consent to Share

- ▶ Qualified Service Organization Agreement
 - Required between JHIE and data contributors
- ▶ Consent must be captured for disclosure of:
 - Addictions information (Part 2)
 - Psychotherapy notes
- ▶ Re-disclosure is not allowed without explicit patient consent



When Consent is Not Required

- ▶ Emergency Setting
 - Must document reason for querying
- ▶ CCOs
 - For TPO, including care coordination and audit/evaluation



Next Steps

- ▶ Behavioral Health Survey
 - EHR Use and capabilities
- ▶ Develop Common Consent Form
 - For use on paper and electronically
- ▶ Document Technical Requirements
- ▶ Behavioral Health Exchange Summit
 - April 12, 2016 (tentative)



JEFFERSON
HEALTH
INFORMATION
EXCHANGE

Break

Security Life Cycle

National Institute of Standards and Technology

Presented by
Carla Raisler



*Privacy is a right that people have;
Security is the protection of that right.*



Carla A. Raisler
ITIL v3, Security+,
CISSP
HealthTech Solutions

Qualifications

Carla is a Certified Information Systems Security Professional

- 15 years of experience in enterprise technology service design, development and implementation
- Extensive experience with IT Security, confidential information, and network architecture
- Expertise in Security and Risk Management, Asset Security, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, HIPAA compliance

NIST is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.

Architecture Description

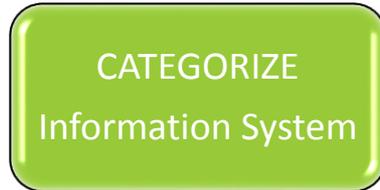
- Business Processes
- FEA Reference Models
- Segment & Solution Architectures
- Information System Boundaries

SP 800-37 / SP 800-53A



Starting Point

FIPS 199 / SP 800-60



Organizational Input

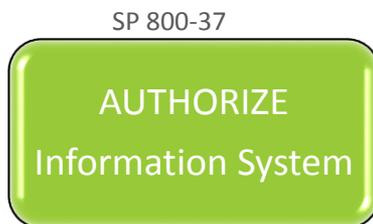
- Laws, Directives, Policy, Guidance
- Strategic Goals and Objectives
- Information Security Requirements
- Priorities and Resources Availability

FIPS 200 / SP 800-53



Security Life Cycle

SP 800-39



SP 800-37



SP 800-70



SP 800-53A

FIPS – Federal Information Processing Standards

FIPS 199 Standards for Security Categorization

FIPS 200 Minimum Security Requirements

SPs – Special Publications

SP 800-60 Mapping Information Types to Security Categories

SP 800-53/53A Security and Privacy Controls catalog/assessment procedures

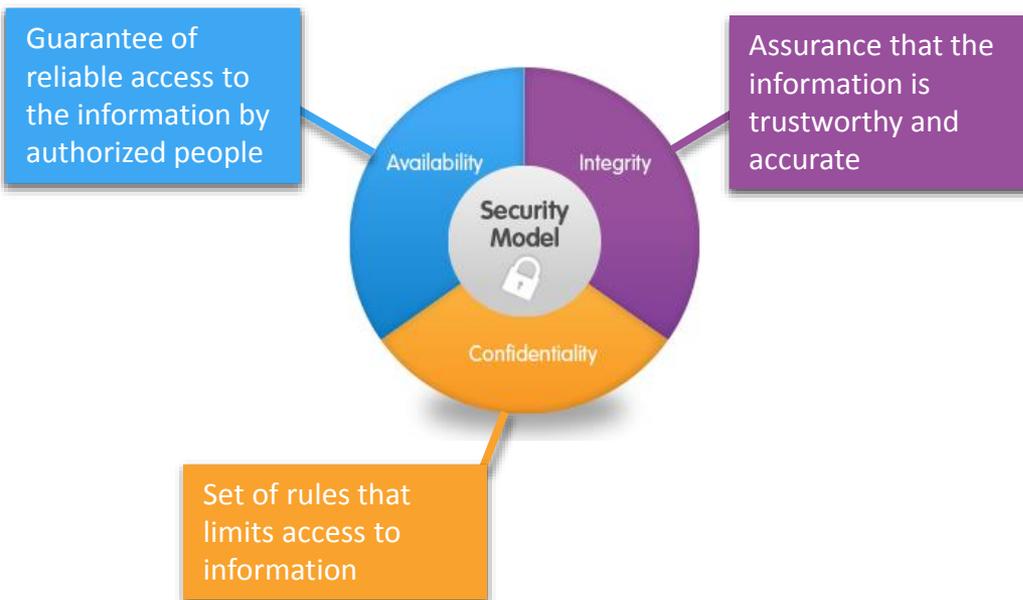
SP 800-70 Security Configuration Checklists Program for IT Products

SP 800-37 Guide for the Security Certification and Accreditation

SP 800-137 Information Security Continuous Monitoring

SP 800-39 Managing Information Security Risk

SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}, where the acceptable values for potential impact are low, moderate, or high.



For impact on information systems, organizations must, as a minimum, employ appropriately tailored security controls from the low, medium, or high baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.

CATEGORIZE: Define criticality/sensitivity of information system according to potential worst-case, adverse impact to business

CATEGORIZE
Information System

NIST 800-53 Security Controls

Control Class	Identifier	Control Family Name	Number of Security Controls
Management	CA	Security Assessment and Authorization	6
	PL	Planning	5
	PM	Program Management	11
	RA	Risk Assessment	4
	SA	System Services and Acquisitions	11
Operational	AT	Awareness and Training	4
	CM	Configuration management	9
	CP	Contingency Planning	9
	IR	Incident Response	8
	MA	Maintenance	6
	MP	Media Protection	6
	PE	Physical and Environmental Protections	18
	PS	Personnel Security	8
	SI	System and Information Integrity	11
	Technical	AC	Access Control
AU		Audit and Accountability	13
IA		Identification and Authentication	8
SC		System and Communications Protection	21
Privacy	AP	Authority and Purpose	2
	AR	Accountability, Audit, and Risk Management	6
	DI	Data Quality and Integrity	2
	DM	Data Minimization and Retention	2
	IP	Individual Participation and Redress	4
	SE	Security	2
	TR	Transparency	2
	UL	Use Limitation	3
TOTAL			197

Management Controls: focus on the management of risk and the management of information system security

Operational Controls: primarily implemented and executed by people

Technical Controls: primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Privacy Controls: promotes closer cooperation between privacy and security officials by establishing a linkage and relationship between privacy and security

SELECT: Select baseline security controls, apply tailoring guidance and suppliant controls as needed based on risk assessment and state laws.

SELECT
Security Controls

CIS Critical Security Controls

- CSC 1: Inventory of Authorized /Unauthorized Devices
- CSC 2: Inventory of Authorized/Unauthorized Software
- CSC 3: Secure Configs for Hardware and Software
- CSC 4: Continuous Vulnerability Assessment/ Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation & Control of Ports, Protocols, & Services
- CSC 10: Data Recovery Capability
- CSC 11: Secure Configurations and Network Devices
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on Need to Know
- CSC 15: Wireless Access Control
- CSC 17: Security Skills Assessment and Training
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20 Penetration Tests and Red Team

P0 security controls are not selected for any baseline

Implement P3 security controls after implementing P2 and P2 controls

Implement P2 security controls after implementing P1 controls

Implement P1 security controls first

Implementation Priorities

IMPLEMENT: implement security controls within enterprise architecture using sound systems engineering practices, apply security configuration settings.

IMPLEMENT
Security Controls

85% of known vulnerabilities can be stopped by deploying the **Top 5 CIS Controls**.

Num.	Control Family
CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges

CSC 1: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

ID	Measure	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
1.1	How many unauthorized devices are presently on the organization's network (by business unit)?	Less than 1%	1%-4%	5%-10%
1.2	How long, on average, does it take to remove unauthorized devices from the organization's network (by business unit)?	60 Minutes	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)
1.3	What is the percentage of systems on the HTS network that are not utilizing Network Level Authentication (NLA) to authenticate to the network	Less than 1%	1%-4%	5%-10%
1.4	How many hardware devices have been recently blocked from connecting to the network by the HTS' NLA			
1.5	How long does it take to detect new devices added to the HTS network?	60 Minutes	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)
1.6	How long does it take to isolate/remove unauthorized devices from HTS' network?	60 Minutes	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)

ASSESS: Determine security control effectiveness (i.e. controls implemented correctly, operating as intended, meeting security requirements for information system.)



85% of known vulnerabilities can be stopped by deploying the **Top 5 CIS Controls**.

Num.	Control Family
CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges

CSC 2: Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

ID	Measure	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
2.1	How many unauthorized software applications are presently located on business systems within HTS	Less than 1%	1%-4%	5%-10%
2.2	How long, on average, does it take to remove unauthorized applications from business systems within HTS	60 Minutes	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)
2.3	What is the percentage of HTS' business systems that are not running software whitelisting software that blocks unauthorized software applications	Less than 1%	1%-4%	5%-10%
2.4	How many software applications have been recently blocked from executing by HTS' software whitelisting software			
2.5	How long does it take to detect new software installed on systems in HTS.	60 minutes	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)
2.6	How long does it take to remove unauthorized software from one of HTS' systems	60 minutes	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)



85% of known vulnerabilities can be stopped by deploying the **Top 5 CIS Controls**.

Num.	Control Family
CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges

CSC 3: Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

ID	Measure	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
3.1	What is the percentage of business systems that are not currently configured with a security configuration that matches HTS' approved configuration standard	Less than 1%	1%-4%	5%-10%
3.2	What is the percentage of business systems whose security configuration is not enforced by HTS' technical configuration management applications	Less than 1%	1%-4%	5%-10%
3.3	What is the percentage of business systems that are not up to date with the latest available operating system software security patches	Less than 1%	1%-4%	5%-10%
3.4	What is the percentage of HTS systems that are not up to date with the latest available business software application security patches	Less than 1%	1%-4%	5%-10%

3.5	How many unauthorized configuration changes have been recently blocked by HTS' configuration management system			
3.6	How long does it take to detect configuration changes to a system	60 Minutes	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)
3.7	How long does it take to reverse unauthorized changes on systems	60 Minutes	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)



85% of known vulnerabilities can be stopped by deploying the **Top 5 CIS Controls**.

Num.	Control Family
CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges

CSC 4: Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

ID	Measure	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
4.1	How many unauthorized devices are presently on the organization's network (by business unit)?	Less than 1%	1%-4%	5%-10%
4.2	What is the average SCAP vulnerability score of each of HTS' business systems			
4.3	What is the total SCAP vulnerability score of each of HTS' business system			
4.4	How long does it take, on average, to completely deploy operating system software updates to a business system	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)	43,200 Minutes (1 month)
4.5	How long does it take, on average, to completely deploy application software updates to a business system?	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)	43,200 Minutes (1 month)

ASSESS
Security Controls

85% of known vulnerabilities can be stopped by deploying the **Top 5 CIS Controls**.

Num.	Control Family
CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges

CSC 5: The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID	Measure	Lower Risk Threshold	Moderate Risk Threshold	Higher Risk Threshold
5.1	How many unauthorized elevated operating system accounts (local administrator/root) are currently? configured on HTS' systems	Less than 1%	1%-4%	5%-10%
5.2	How many unauthorized elevated application accounts are currently configured on HTS' systems?			
5.4	What percentage of HTS' elevated accounts do not require two-factor authentication?	Less than 1%	1%-4%	5%-10%
5.5	How many attempts to upgrade and account to administrative privileges have been detected on HTS' systems recently?			
5.6	How many attempts to gain access to password files within the system have been detected on HTS' systems recently			
5.7	How long does it take for administrators to be notified about user accounts being added to super user groups	60 Minutes	1,440 Minutes (1 Day)	10,080 Minutes (1 Week)



Plan of Action and Milestones

- Plan to correct vulnerabilities
- Resources requires to accomplish the task

Security Authorization Package

- Security Plan
- Security Assessment
- Plan of action and milestones

Risk Determination

- How risks are assessed with the organization
- Risk mitigation approach
- How risk will be monitored

Risk Acceptance

- Authorization to operate
- Terms and conditions of operation

AUTHORIZE: Determine risk to organizational operations and assets, individuals, other organizations, and the Nation, if acceptable, authorize operation.

AUTHORIZE
Information System

Determine the security impact of proposed or actual changes to the information system and its environment of operation.

Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

Conduct remediation actions based on the results of ongoing monitoring

Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

Implement an information system decommissioning strategy

Report the security status of the information system to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.

Review the reported security status of the information system



MONITOR: Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

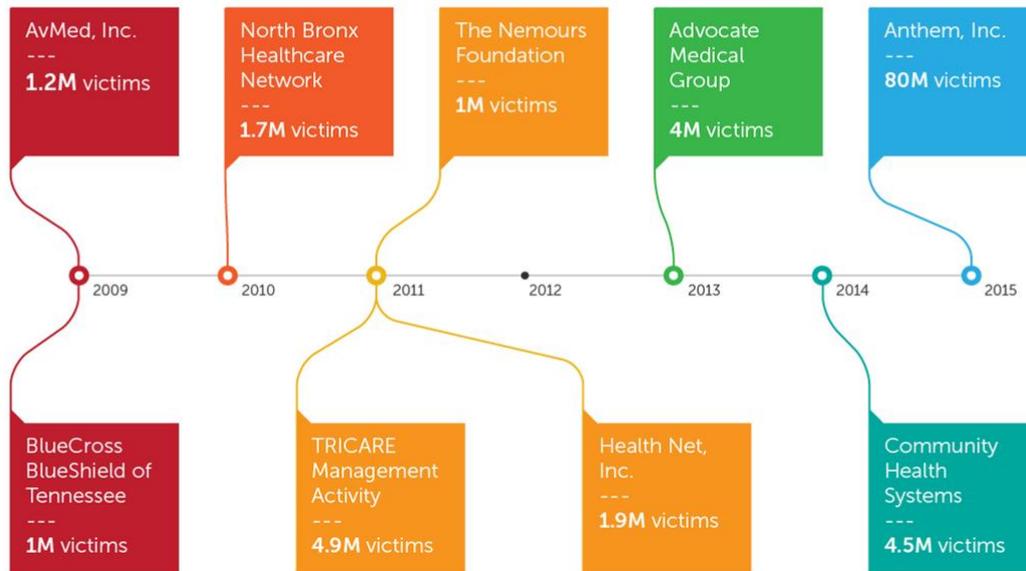
MONITOR
Security Controls

"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012



NOTABLE HEALTHCARE BREACHES



KEY FINDINGS

- 92% of breaches were performed by external attackers
- 75% were untargeted and opportunistic
- 78% used tactics rated as low or very low on the VERIS difficulty scale
- 75% were driven by financial motives
- 19% were perpetrated by state affiliated actors for espionage
- 38% impacted larger organizations
- 52% involved some form of hacking
- 40% incorporated malware
- 54% compromised servers
- 66% were detected months or years after the initial compromise
- Only 9% were detected by resources within the affected organization

Data Breach



2015 Data Breach Investigation Report: <http://www.verizonenterprise.com/DBIR/2015/>

OCR Breach Notifications: <https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-SECURITY-LIST&a=1>



November 25, 2015

HIPAA SETTLEMENT REINFORCES LESSONS FOR USERS OF MEDICAL DEVICES

Lahey Hospital and Medical Center (Lahey) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules with the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR). Lahey will pay \$850,000 and will adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Lahey is a nonprofit teaching hospital affiliated with Tufts Medical School, providing primary and specialty care in Burlington, Massachusetts.



November 30, 2015

Triple-S Management Corporation Settles HHS Charges by Agreeing to \$3.5 Million HIPAA Settlement

Triple-S Management Corporation (“TRIPLE-S”), on behalf of its wholly owned subsidiaries, Triple-S Salud Inc., Triple-C Inc. and Triple-S Advantage Inc., formerly known as American Health Medicare Inc., has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR). TRIPLE-S will pay \$3.5 million and will adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program, an effort it has already begun.

December 14, 2015

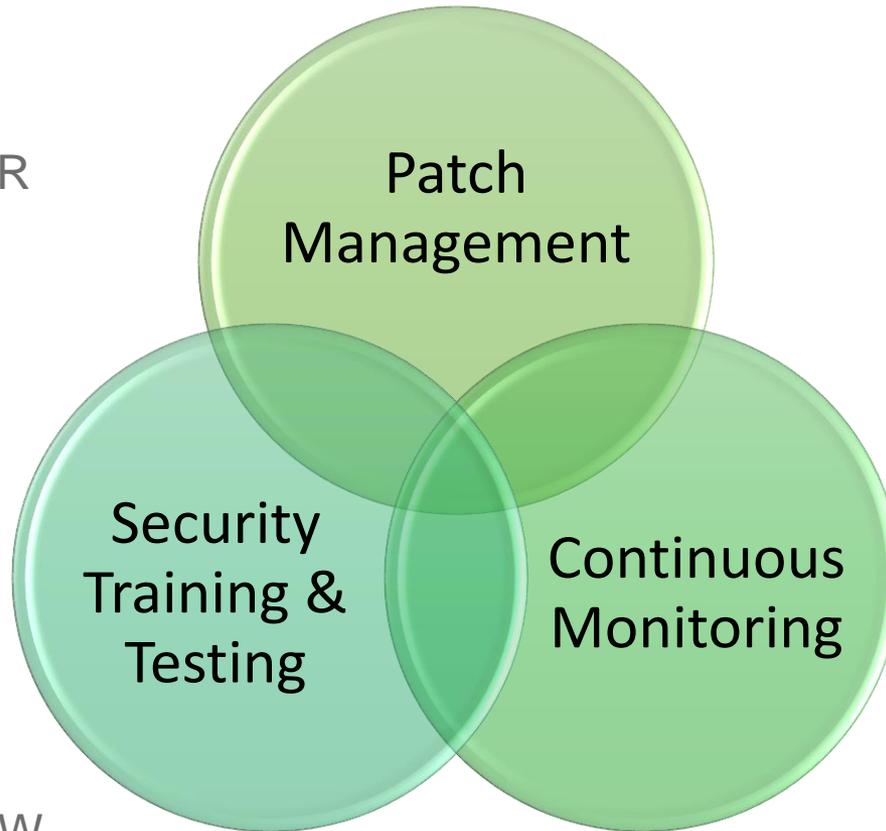
**\$750,000 HIPAA SETTLEMENT UNDERSCORES THE NEED FOR ORGANIZATION WIDE
RISK ANALYSIS**

The University of Washington Medicine (UWM) has agreed to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule by failing to implement policies and procedures to prevent, detect, contain, and correct security violations. UWM is an affiliated covered entity, which includes designated health care components and other entities under the control of the University of Washington, including University of Washington Medical Center, the primary teaching hospital of the University of Washington School of Medicine. Affiliated covered entities must have in place appropriate policies and processes to assure HIPAA compliance with respect to each of the entities that are part of the affiliated group. The settlement includes a monetary payment of \$750,000, a corrective action plan, and annual reports on the organization's compliance efforts.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) initiated its investigation of the UWM following receipt of a breach report on November 27, 2013, which indicated that the electronic protected health information (e-PHI) of approximately 90,000 individuals was accessed after an employee downloaded an email attachment that contained malicious malware. The malware compromised the organization's IT system, affecting the data of two different groups of patients: 1) approximately 76,000 patients involving a combination of patient names, medical record numbers, dates of service, and/or charges or bill balances; and 2) approximately 15,000 patients involving names, medical record numbers, other demographics such as address and phone number, dates of birth, charges or bill balances, social security numbers, insurance identification or Medicare numbers.

99.9%

OF THE EXPLOITED
VULNERABILITIES
WERE
COMPROMISED
MORE THAN A YEAR
AFTER THE CVE
WAS PUBLISHED.



256 Days

Malicious attacks can take an average of 256 days to identify while data breaches caused by human error take an average of 158 days to identify

23%

OF RECIPIENTS NOW
OPEN PHISHING
MESSAGES AND
11% CLICK ON
ATTACHMENTS.



Carla A. Raisler
ITIL v3, Security+, CISSP
HealthTech Solutions
Carla.raisler@healthtechsolutions.com

*“Privacy is a right that people have;
Security is the protection of that right.”*

HITOC Charter, Workplan, and Priorities

Susan Otter
Justin Keller

The logo for the Oregon Health Authority. It features the word "Oregon" in a smaller, orange, serif font positioned above the word "Health". "Health" is written in a large, dark blue, serif font. Below "Health", the word "Authority" is written in a smaller, orange, serif font. A thin blue horizontal line is positioned just above the "Authority" text, extending from the left side of the "H" in "Health" to the right edge of the "Authority" text.

Oregon
Health
Authority

Goals of HIT-Optimized Health Care

1. Sharing Patient Information Across the Care Team

- Providers have access to meaningful, timely, relevant and actionable patient information to coordinate and deliver “whole person” care.

2. Using Aggregated Data for System Improvement

- Systems (health systems, CCOs, health plans) effectively and efficiently collect and use aggregated clinical data for quality improvement, population management and incentivizing health and prevention.
- In turn, policymakers use aggregated data and metrics to provide transparency into the health and quality of care in the state, and to inform policy development.

3. Patient Access to Their Own Health Information

- Individuals and their families access their clinical information and use it as a tool to improve their health and engage with their providers.

Aims & Objectives

Goal 1 of “HIT-Optimized Health Care”: Providers have access to meaningful, timely, relevant and actionable patient information to coordinate and deliver “whole person” care

Provider role in support of “HIT-Optimized Health Care”: have the technology capabilities and workflows to participate in care coordination, including: (1) Pursue meaningful use of HIT (particularly for those eligible for EHR Incentive Programs); (2) Participate in care coordination and health information exchange that is inclusive of all members of the care team

1. Increased adoption of standards-based technology for data capture, use, and exchange
2. Improved ability to capture, produce and use interoperable standards-based data in formats that are structured to be integrated and automated within EHRs and workflows
3. Improved access to and sharing of meaningful patient information across organizational and technological boundaries
4. Ensured protection of privacy and security of patient information
5. Improved provider experience and workflows, reduced burden and increased workforce capacity

Aims & Objectives

Goal 2 of “HIT-Optimized Health Care”: Systems effectively and efficiently collect and use aggregated clinical data for quality improvement, population management, and incentivizing health and prevention

Systems’ (e.g., CCOs, Health Plans) role/responsibility in support of “HIT-Optimized Health Care”: (1) Implement HIT tools for data collection, processing, and reporting; (2) Align clinical metric reporting requirements with meaningful use clinical quality measures; (3) Encourage and support meaningful use and health information exchange among contracted providers

1. Improved use of HIT tools for data collection, analytics, and reporting
2. Increased use of aggregated data, including clinical data for population management, quality improvement, and alternative payment methods
3. Reduced reporting burden for clinical metrics across programs

Aims & Objectives

Goal 3 of “HIT-Optimized Health Care”: Individuals and their families access their clinical information and use it as a tool to improve their health and engage with their providers

Individuals’ and families’ role/responsibility in support of “HIT-Optimized Health Care”: (1) Expect providers to have electronic access to their relevant information; (2) Inform providers where they can access patient-generated information (e.g. personal health record); (3) Access their health records via available patient portals; (4) Communicate electronically with providers.

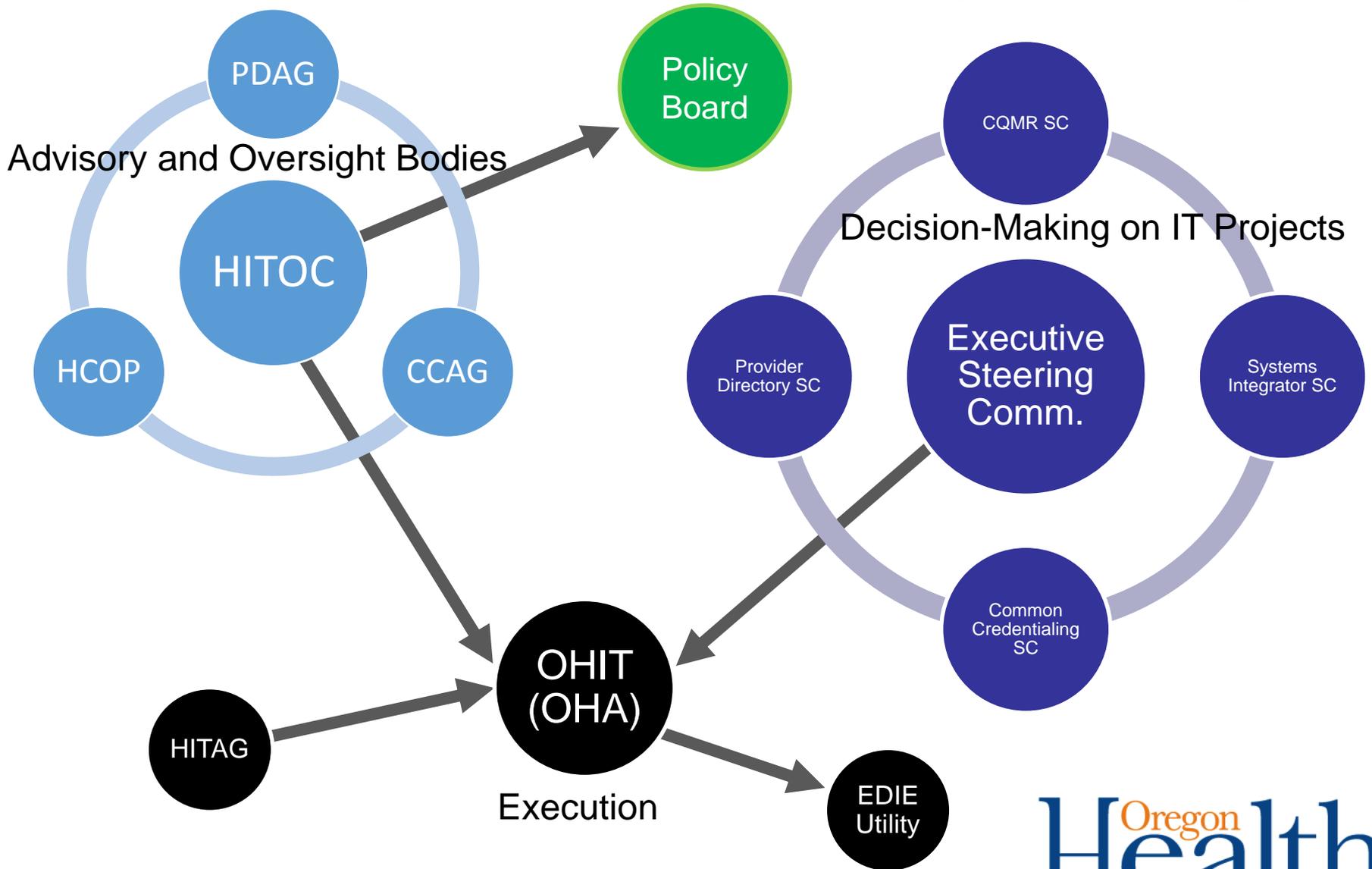
1. Increased patient access to/use of their complete health records
2. Improved ability for individuals to provide important information into their health records
3. Increased capacity for individuals to facilitate care management by sharing information with their providers
4. Ensured confidence in the privacy and security of electronic health information

HITOC & HCOP

- Identify opportunities for HITOC to consider regarding providing guidance and/or developing policy to address barriers or better support HIT/HIE efforts in Oregon



Health IT Governance “Galaxy” in Oregon



Charter – Responsibilities of HITOC

- Make recommendations related to Health IT to the Board to achieve the goals of health system transformation
 - Strategic plans for health IT; policy priorities and/or barriers
 - Respond to Board requests
- Regularly review and report to the Board on:
 - OHA health IT efforts including the Oregon Health IT program toward achieving goals of health system transformation
 - Efforts of local, regional, and statewide organizations to participate in health IT systems
 - Progress related to adoption and use of health IT among providers, systems, patients, and other users in Oregon
- Advise the Board or the Congressional Delegation on federal law and policy changes that impact health IT efforts in Oregon

HITOC Membership

Name	Title	Organizational Affiliation	Location
Richard (Rich) Bodager, CPA, MBA	CEO/Board Chair	Southern Oregon Cardiology/Jefferson HIE	Medford, OR
Maili Boynay	IS Director Ambulatory Community Systems	Legacy Health	Portland, OR
Robert (Bob) Brown	Retired Advocate	Allies for Healthier Oregon	Portland, OR
Erick Doolen	COO	PacificSource	Springfield, OR
Chuck Fischer	IT Director	Advantage Dental	Redmond, OR
Valerie Fong, RN	CNIO	Providence Health & Services	Portland, OR
Charles (Bud) Garrison	Director, Clinical Informatics	Oregon Health & Science University	Portland, OR
Brandon Gatke	CIO	Cascadia Behavioral Healthcare	Portland, OR
Amy Henninger, MD	Site Medical Director	Multnomah County Health Department	Portland, OR
Mark Hetz	CIO	Asante Health System	Medford, OR
Betty Kramp, RN	Clinical Applications Coordinator	United States Public Health Service (Currently: Indian Health Services, Klamath Tribal Health & Family Svcs)	Chiloquin, OR
Jim Rickards, MD	Health Strategy Officer	Yamhill Community Care Organization	McMinnville, OR
Sonney Sapra	CIO	Tuality Healthcare	Hillsboro, OR
Greg Van Pelt	President	Oregon Health Leadership Council	Portland, OR

High Level Work Plan

2016

2017

Policy Topics	<ul style="list-style-type: none"> • Interoperability • Behavioral Health Information Sharing • Other Policy Board or HITOC-identified Topics • Chartered Committee Policy Work 			<ul style="list-style-type: none"> • Identifying new priorities for 2017-2019 biennium
Strategic Planning	<ul style="list-style-type: none"> • Rely on Existing Business Plan Framework 	<ul style="list-style-type: none"> • Process to develop next HIT strategic plan 	<ul style="list-style-type: none"> • Release of next strategic plan 	
Oversight	<ul style="list-style-type: none"> • Consideration of pressing issues as <u>Oregon HIT Program</u> develops • Regular staff updates 			
HIT Environment and Reporting	<ul style="list-style-type: none"> • Define scope of environmental scan • Define format and scope of HITOC Reporting to Board • First Report to the Policy Board due June 2016 	<ul style="list-style-type: none"> • First Report to the Legislature on Oregon HIT Program released Summer 2016 	<ul style="list-style-type: none"> • Second Report to the Board due Winter 2016-2017 	<ul style="list-style-type: none"> • Second Report to Legislature on OR HIT Program released Summer 2017
Federal Policy	<ul style="list-style-type: none"> • Federal Law/Policy Considerations (e.g. Meaningful Use; ONC Interoperability roadmap, ONC standards advisory, privacy and security requirements (42 CFR part 2, etc.)) 			

HITOC-HCOP Relevant Topic Areas

- Barriers to interoperability and health information exchange
- Consent and privacy issues
- 42 CFR Part 2 and behavioral health sharing
- Governance and financing models
- Sample data sharing agreements, including data use and privacy/security

HITOC Feedback on HCOP

- HITOC members were curious about consumer representation on HCOP
- Endorsed HCOP Charter

Preview: Behavioral Health Information

- ONC Cooperative Agreement awarded to OHA and sub-recipient Jefferson HIE
- Objectives:
 - Develop universal interpretation of law for exchange, disclosure, and re-disclosure of drug, alcohol and mental health data in Oregon (e.g., 42 CFR Part 2)
 - Develop a common consent management model
 - Implement consent model within Jefferson HIE technology
 - Connect with behavioral health EHRs and others
- HITOC work ahead/discussion:
 - Jefferson HIE to orient HITOC to their work
 - OHA Behavioral Health provider survey
 - Consider workgroup or sub-committee

Preview: Interoperability

- Improving interoperability across HIT/HIE investments
 - Identify barriers, priorities for interoperability
 - Support providers, stakeholders in navigating interoperability
- Potential work products for HITOC:
 - Data collection/environmental scan on interoperability in Oregon,
 - Guidelines or principles for HIT/HIE participants in Oregon
 - Compatibility Program: expectations for users of state HIT services
 - HIT vendor interoperability scorecard
- HITOC work ahead/discussion:
 - Scope and charter this work
 - Consider workgroup or sub-committee
 - Identify subject matter expertise needed

Interoperability SME Workgroup

- Intention is to have a group that supports OHA in developing the agenda around interoperability for HITOC
- Overlap between SME Workgroup and HCOP:
 - Flagging for OHA critical policy barriers to real-world interoperability
 - Flagging for OHA/HITOC important opportunities and levers for the state
 - Validating the work of the SME Workgroup as the “boots-on-the-ground” group
 - Other option: merge SME Workgroup with HCOP
- Next Steps: Bring a draft charter to HITOC in February

Break

Roundtable

- Brief Update
- Successes
- Challenges

HCOP Future Topics

- Cyber Security

Conclusions, Next Meeting, and Action Items

- HCOP to continue meeting quarterly in 2016
 - April 14th 1-5 pm
 - July 12th 1-5 pm
 - October 14th 1-5 pm

Process Check

- What did you like about this meeting?
 - Format?
 - Activities?
 - Discussion?
- What would you like to see us change?
 - What should we add?
 - What should we remove?

For more information on Oregon's HIT/HIE developments,
please visit us at <http://healthit.oregon.gov>

Susan Otter, Director of Health Information Technology
Susan.Otter@state.or.us

Marta Makarushka, Strategy and Policy Analyst
Marta.M.Makarushka@state.or.us

