



Implementing Role Based Access Control (RBAC) in Healthcare

Draft Standard for Trial Use,
Adoption and Interoperability between
Standards Organizations

Role Based Access Control - RBAC

- **Role-Based Access Control** (RBAC) is a type of policy based access control where entity access is granted based upon membership in a group (role) and where rights and privileges are bestowed upon the role rather than the entity directly.
- **Goals**
 - Mechanism for scalable management of user permissions in the form of operations and objects
 - Support interoperability among healthcare and non-healthcare partners
 - Provide information accessibility on a “need-to-know” basis

Role Based Access Control

- Enterprise-wide set of roles that would be compatible across a portfolio of applications
- Interoperability of access control among the VHA and its business partners.*

* This implies a degree of standardization within the healthcare community.

RBAC Development

- Creation of National RBAC Task Force (RBAC TF)
- Selection of ASTM Standard E1986-98, Standard Guide for Information Access Privileges to Health Information used for basic role names
- Adoption of previous HL7 Technical Committee work, storyboards
- Adoption of facilitated sessions of the VHA RBAC TF

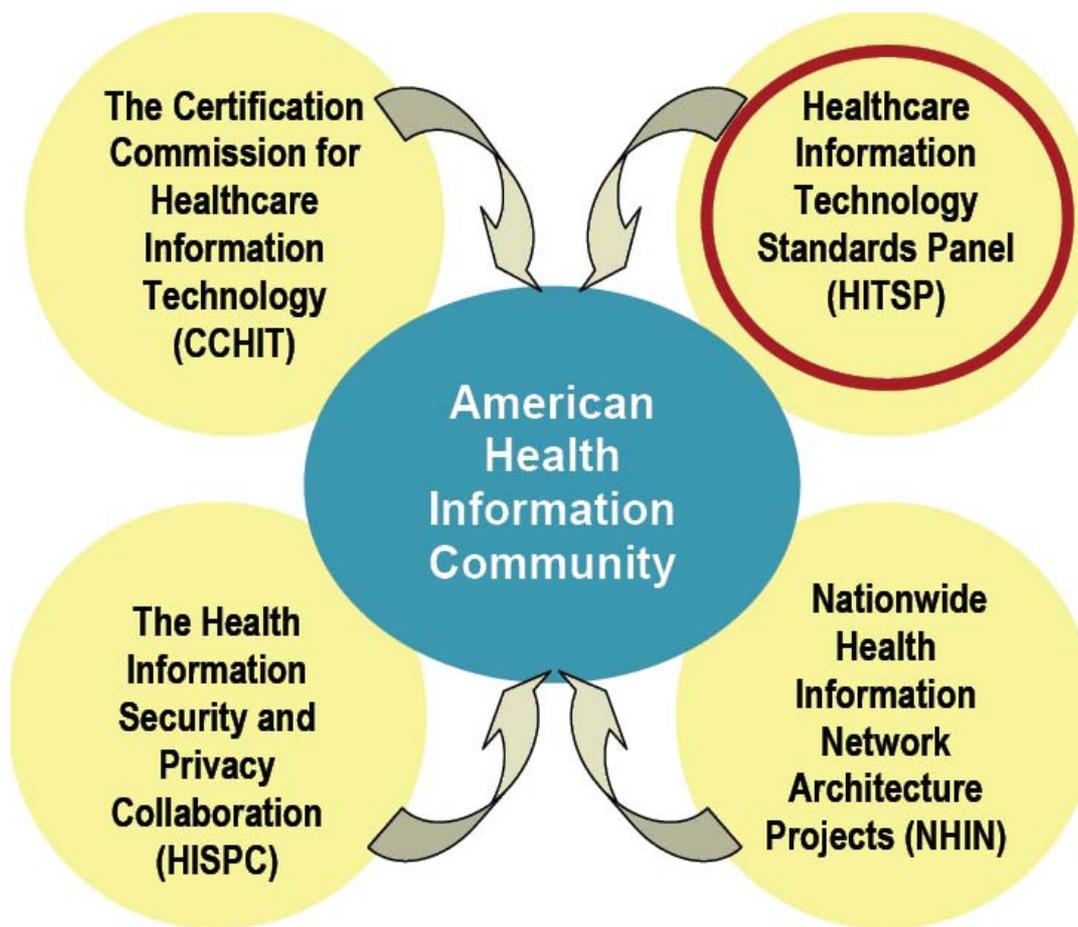
Role Engineering

- ACTION 1: Identify and Model Usage Scenarios
- ACTION 2: Permission Derivation from Scenarios
- ACTION 3: Identification of Permission Constraints
- ACTION 4: Scenario Model Refinement
- ACTION 5: Definition of Tasks and Work Profiles
- ACTION 6: Derivation of a Preliminary Role-hierarchy
- ACTION 7: RBAC Model Definition

Integrating RBAC in SDO Activities



A public-private "Community" is created as the focal point for America's health information concerns and to drive opportunities for increasing interoperability



HITSP includes 348 different member organizations and is administered by a Board of Directors

24 SDOs (7%)
247 Non-SDOs (71%)
30 Govt. bodies (9%)
12 Consumer groups (3%)
36 Project Team and Undeclared (10%)

*The **Community** is a federally-chartered commission and will provide input and recommendations to HHS on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected, in a smooth, market-led way.*

HL7 Draft Standard for Trial Use

- HL7 RBAC Role Engineering Process
- HL7 RBAC Healthcare Scenarios*
(derived from ASTM 1986E Documentation)
- HL7 RBAC Healthcare Permission Catalog*
- HL7 Healthcare Scenario Roadmap

* developed with subject matter experts from VHA, IHS, Kaiser, DoD collaborative RBAC Task Force

RBAC Lightweight Process

- The purpose of the Lightweight Process is to accompany the document 'VHA RBAC Role Engineering Process.'
- This process is a brief guide to be used by security engineers, subject matter experts, and others involved in defining roles for VHA.

Healthcare Relationships

In Healthcare, allowable permissions for users are similar, for example:

- Create a new pharmacy order
- Read a new medication order
- Update a medication order
- Delete a medication* *

Healthcare Permissions

Scenario ID	Unique Permission ID	Abstract Permission Name	Basic Permission Name {Operation, Object}
SOE-002	POE-001	New Laboratory Order	{C, Laboratory Order}
SOE-002	POE-002	Change/Discontinue Laboratory Order	{U, Laboratory Order}
SOE-001	POE-003	New Radiology Order	{C, Radiology Order}
SOE-007	POE-004	Change/Discontinue Radiology Order	{U, Radiology Order}
SOE-001	POE-005	New/Renew Outpatient Prescription Order	{C, Outpatient Prescription Order}
SOE-001	POE-006	Change/Discontinue/Refill Outpatient Prescription Order	{U, Outpatient Prescription Order}

Healthcare Scenario Roadmap

Permission ID	Scenario ID	Basic Permission Name {Operation, Object}	Task and Step	Legend:													
				Licensed Healthcare Providers	Audiologist	Dental Hygienist/Registered Dental Hygienist (RDH)	Dentist (DDS or DMD)	Dentist	Oral Surgeon	Dietitian (RD)	Non-western Medicine Providers	Certified Acupuncturist (CA)	Licensed Massage Therapist (LMT)/Registered Massage Therapist (RMT)	Nurse	Clinical Nurse Specialist (CNS)	Clinical Registered Nurse Anesthetist (CRNA)	
		<p>C = Create R = Read U = Update D = Delete E = Execute</p>	<p>Legend: x = performs o = does not perform ? = unknown</p> <p>Green highlight = Changes immediately after Task Force approval Yellow highlight = Pending Task Force review and approval Red highlight = Deferred Purple highlight = In progress</p>														
			Order Entry														
POE-001	SOE-002	{C, Laboratory Order}	New Laboratory Order					x	x	x						x	x
POE-002	SOE-002	{U, Laboratory Order}	Change/Discontinue Laboratory Order					x	x	x						x	x
POE-003	SOE-001	{C, Radiology Order}	New Radiology Order					x	x							x	x
POE-004	SOE-007	{U, Radiology Order}	Change/Discontinue Radiology Order					x	x							x	x
POE-005	SOE-001	{C, Outpatient Prescription Order}	New/Renew Outpatient Prescription Order					x	x	x						x	x
POE-006	SOE-001	{U, Outpatient Prescription Order}	Change/Discontinue/Refill Outpatient Prescription Order					x	x	x						x	x
POE-007	SOE-003	{C, Inpatient Medication Order}	New Inpatient Medication Order					x	x							x	x
POE-008	SOE-003	{U, Inpatient Medication Order}	Change/Discontinue Inpatient Medication Order					x	x							x	x
POE-009	SOE-002	{C, Diet Order}	New Diet Order					x	x	x						x	x
POE-010	SOE-002	{U, Diet Order}	Change/Discontinue Diet Order					x	x	x						x	x
POE-011	SOE-001	{C, Consult Order}	New Consult Order		x			x	x	x						x	x
POE-012	SOE-006	{U, Consult Order}	Change/Discontinue Consult Order		x			x	x	x						x	x
POE-013	SOE-003	{C, Nursing Order}	New Nursing Order					x	x	x						x	x
POE-014	SOE-003	{U, Nursing Order}	Change/Discontinue Nursing Order					x	x	x						x	x
POE-015	SOE-002	{C, Standing Order(s) PRN}	New Standing Order(s) PRN					x	x	x						x	x

Healthcare Constraints

Role Based access control can be adjusted to work with a healthcare system.

Permissions can be added or subtracted from entire user roles to adjust for changes in policy within the system.

Reduce Overall Management Costs

- Reduces complexity and cost of security administration in large networked applications in areas ranging from healthcare to defense in addition to mainstream commerce systems
- RBAC maps to organizational-specific structures in a way that reduces direct and indirect admin costs and improves security
- Simplified systems administration
- Enhanced organizational productivity
- Reduction in new employee downtime
- Enhanced systems security & integrity
- Simplified regulatory compliance

Reduce Overall Access Management Costs

Users change often, roles do not.

Contact Information

RBAC Website: www.va.gov/RBAC

Mike Davis, VHA OI&T Security Architect
(760) 632-0294
Mike.Davis@va.gov

Suzanne Gonzales-Webb, CPhT
SAIC Information Security Analyst
VHA OI&T Senior Systems Engineer
(858) 826-6621
suzanne.l.gonzales-webb@saic.com
suzanne.gonzales-webb@va.gov