

VHA

HEALTH INFORMATION
ARCHITECTURE

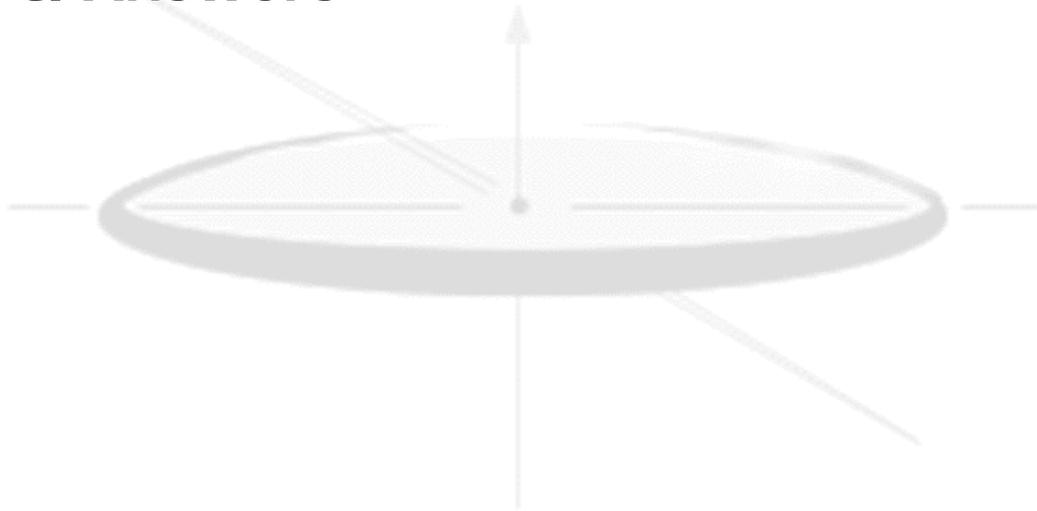
CyberSec – User Authorization with Role-Based Access Control (4454)

RBAC

VA ITC
Austin, Texas
August 10, 2004

Outline

- **Security** – Steven Wagner, VHA Security Architect
- **RBAC Task Force** – Dr. Robert O’Hara & Dawn Rota, RN
- **RBAC Workgroup** – Chuck Brown, Program Manager
- **Questions & Answers**



Security

Security Problem Description

- **Complexity** - Multiple different systems, protocols and implementations
- **Scalability** - Hundreds of systems and tens of thousands of users, millions of Veterans
- **Adaptability** - New policies and practices not originally planned, new technologies
- **Interoperability** - Secure data exchange with business partners
- **Assurability** - Certification, testing and maintaining assurance of security function over system life-cycle

The Solution: AAIP

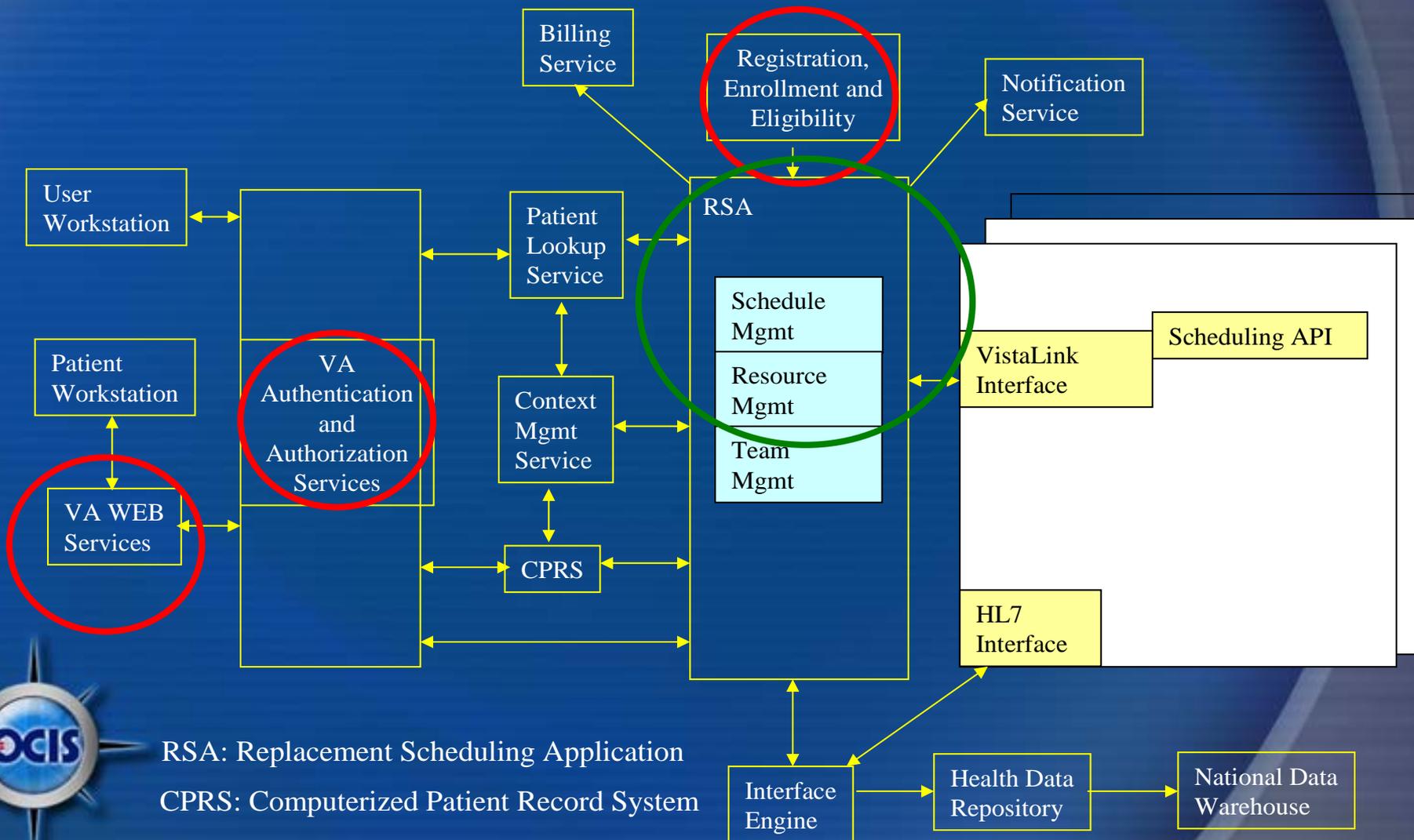
The Department's **Authentication and Authorization Infrastructure Project (AAIP)** under OCIS will provide a common security infrastructure for identity and access management that allows for sharing of security information and “decouples” security mechanisms that are tightly integrated with specific applications.

Parties



- *Who are the stakeholders?*
 - **VA employees (IT, security, architects, designers, developers and users)**
 - **Patients**
 - **Business partners**
- *Who within VA is responsible?*
 - **OCIS**
 - **VHA RBAC TF**
 - **Developers**
 - **Management**
- *Who is VHA collaborating with to accomplish this?*
 - **IHS, DoD, Kaiser Permanente, AAMC, Standards Development Organizations (HL7, ASTM, OASIS)**

EA Example Diagram



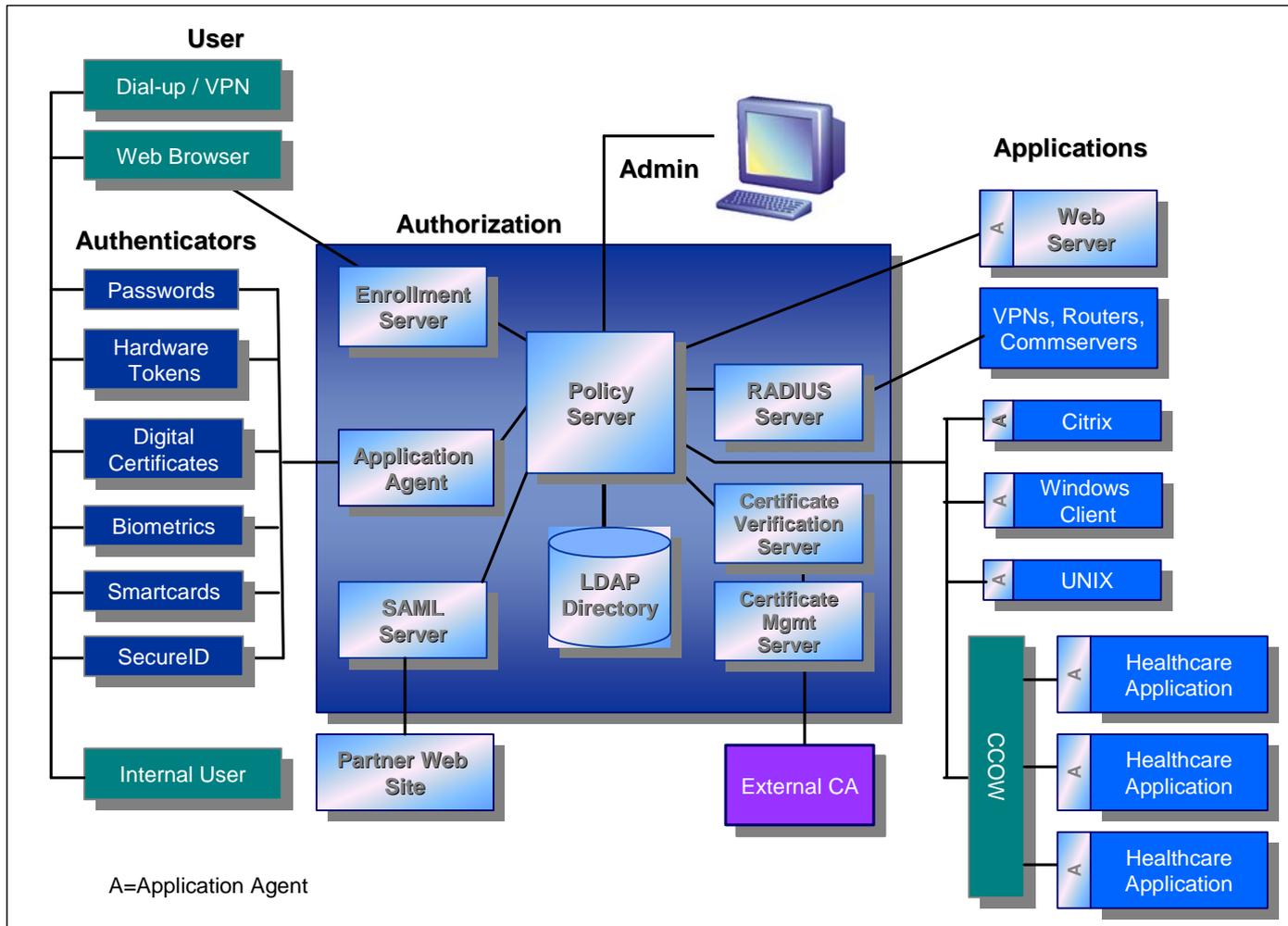
Role-Based Access Control

- 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.

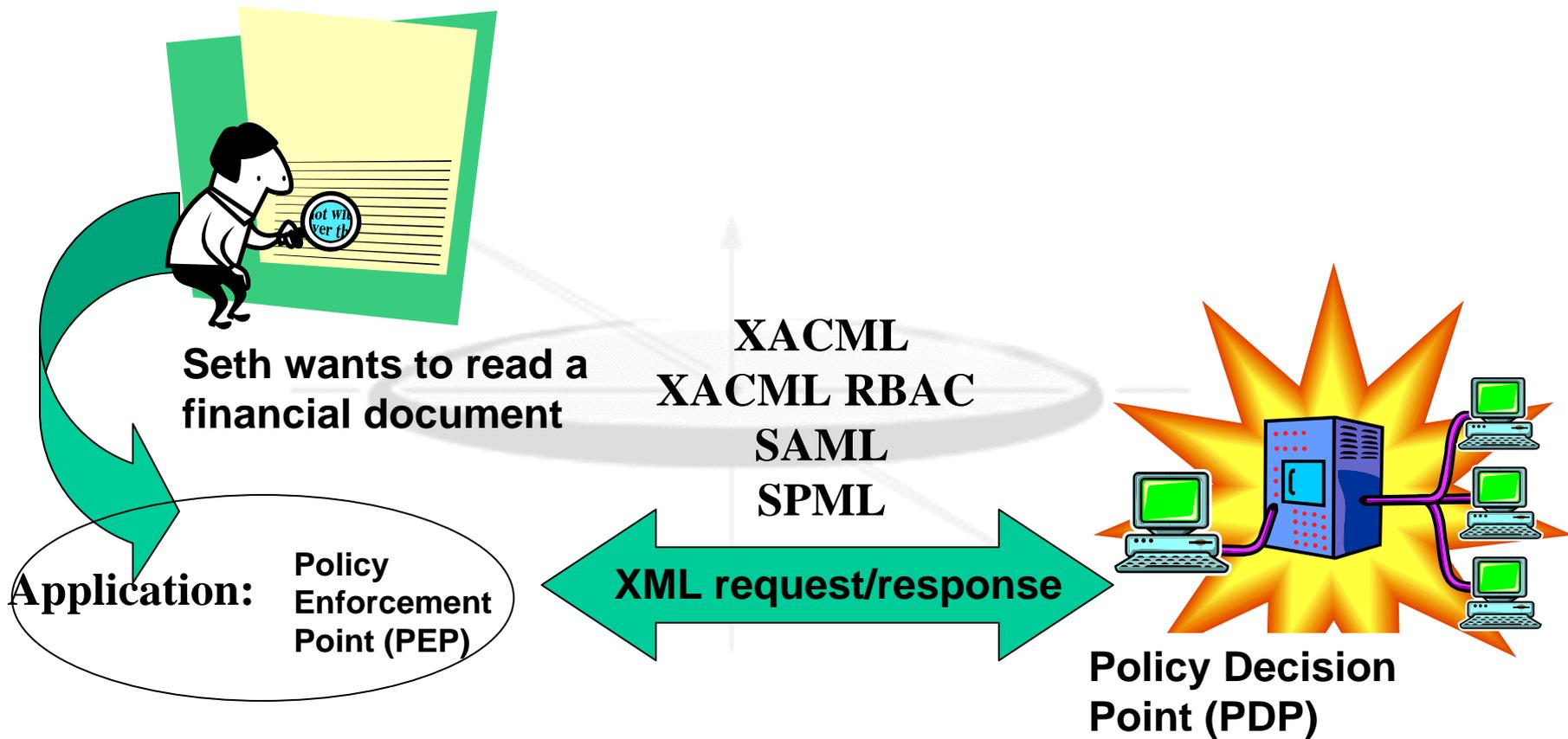
RBAC Is Essential to AAIP Access Management

- “Only authorized personnel will be approved for access to VA information systems...approval must be specific to each individual’s roles and responsibilities in the performance of duties...” [VA Handbook 6500]
- Role-based access control (RBAC) is particularly useful in healthcare environments with user roles and access requirements such as separation of duties. [ASTM 1986]
- AAIP infrastructure must be in place before RBAC can be supported.
- Roles must be defined before RBAC can be used on an enterprise basis. Administrations manage and define roles

Authorization Framework



Example: Making a Role Request Using XML Protocols



AAIP Authorization Framework Support for VHA Requirements

- Support for the full range of VHA health information system topologies (CCOW, Thin Client, Web, etc.).
- Place AA services at the Enterprise level.
- Support medical sign-on, persistent sessions.
- Support Enterprise and Federated SSO.
- Support Emergency Access.
- Provide for Federated identity management.
- Provide Enterprise-wide user profiles and attributes.
- Provide support to healthcare roles.
- Support application level authentication, authorization and delegation.
- Provide centralized security administration.
- Support for healthcare standards/interoperability.

AAIP Benefits

- Solves Department's security scalability problems with One-VA AA infrastructure
- Simplifies authorization management
- Reduces administrative costs
- Improves security
- Enhances business partner interoperability
- Enables new network-level RBAC services
- Improves service to members/clients/patients

RBAC Task Force



Some RBAC Milestones

Aug 2003	Initial VHA Requirements to AAIP
Oct 2003	VHA Basic Roles Provided to AAIP
May 2004	HL7 Begin Define RBAC Permissions
Sep 2004	Begin AAIP PKI Deployment
Aug 2004	New RBAC TF
Aug 2004	VHA-OCIS AAIP Meeting
Sep 2004	VHA Requirements for AAIP vetted
Sep 2004	RSA Project LDAP Architecture
Sep 2005	VHA Functional Roles Defined
Jan 2005	Begin Access Mgt Pilot
Sep 2006	AAIP PKI Deployment Complete
Sept 2005	AAIP Access Management Component
Sep 2005	HL7 Initial Permission Catalog

VHA/IHS RBAC TF Objectives

- Define a healthcare industry-wide permission catalogue standard.
- Define the healthcare permission content for the VA OCIS Authentication and Authorization Infrastructure Project (AAIP).
- Integrate RBAC model into Health eVet-VistA.
- Teach the RBAC Role Engineering Process to new VHA software projects and identify permissions during development.
- Collaborate with IHS and Standards Development Organizations (SDOs) to support interoperability.
- Collaborate with other interested enterprises, including DoD, Kaiser Permanente and international.

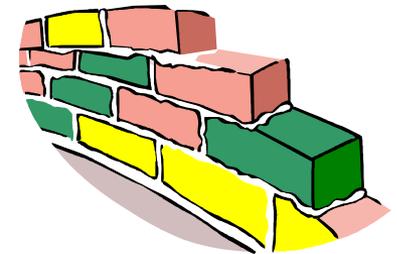
How They All Fit Together

ROLE = Physician



Dr. Joe Smith is an
Oncologist

PERMISSION = Write Medication Order

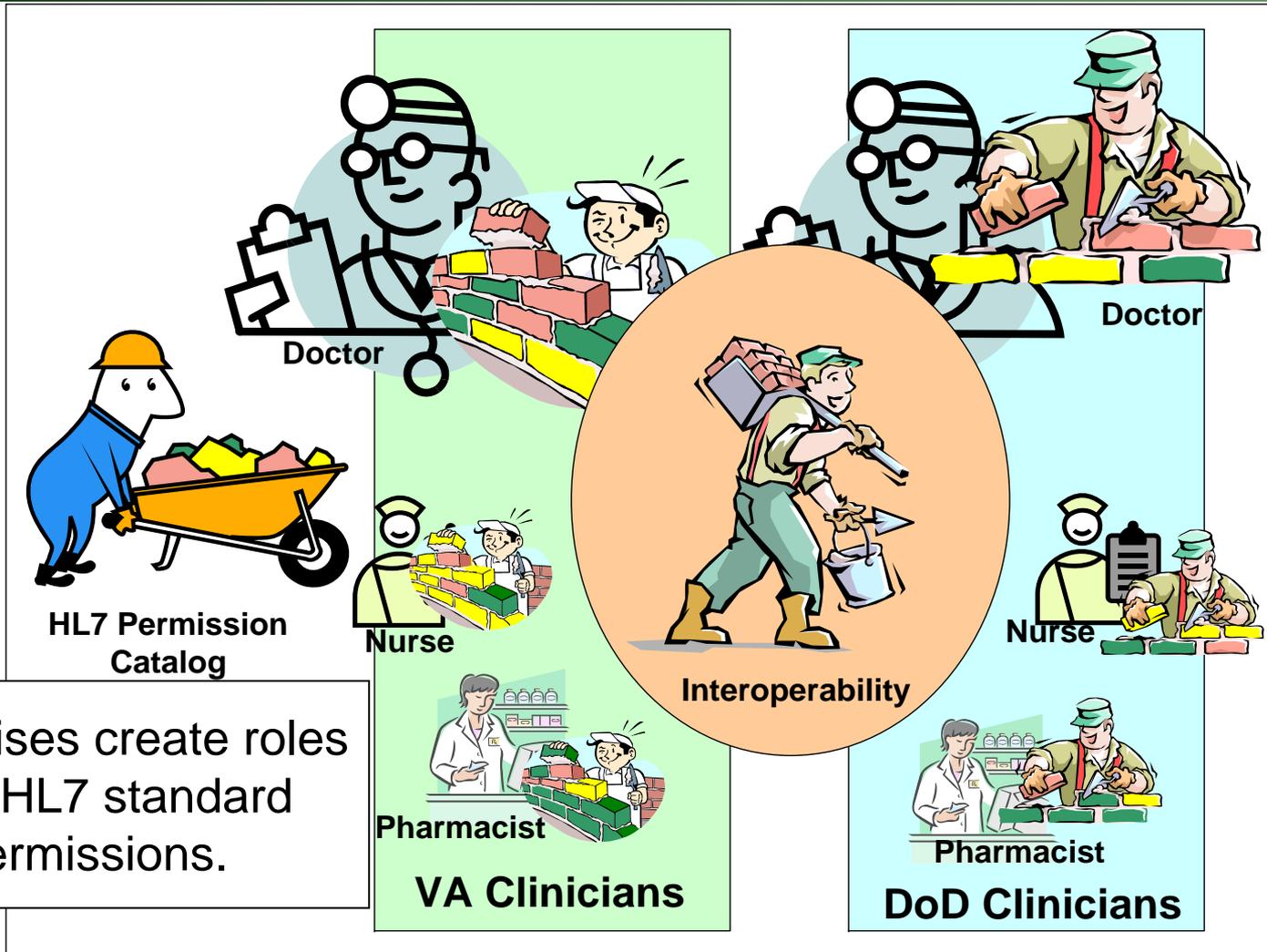


BUSINESS RULE = Oncologists may Write
"Chemotherapy" Medication Orders

CONSTRAINT = 1st year Oncology Residents
need Chemotherapy Medication Orders
co-signed by an Attending Physician

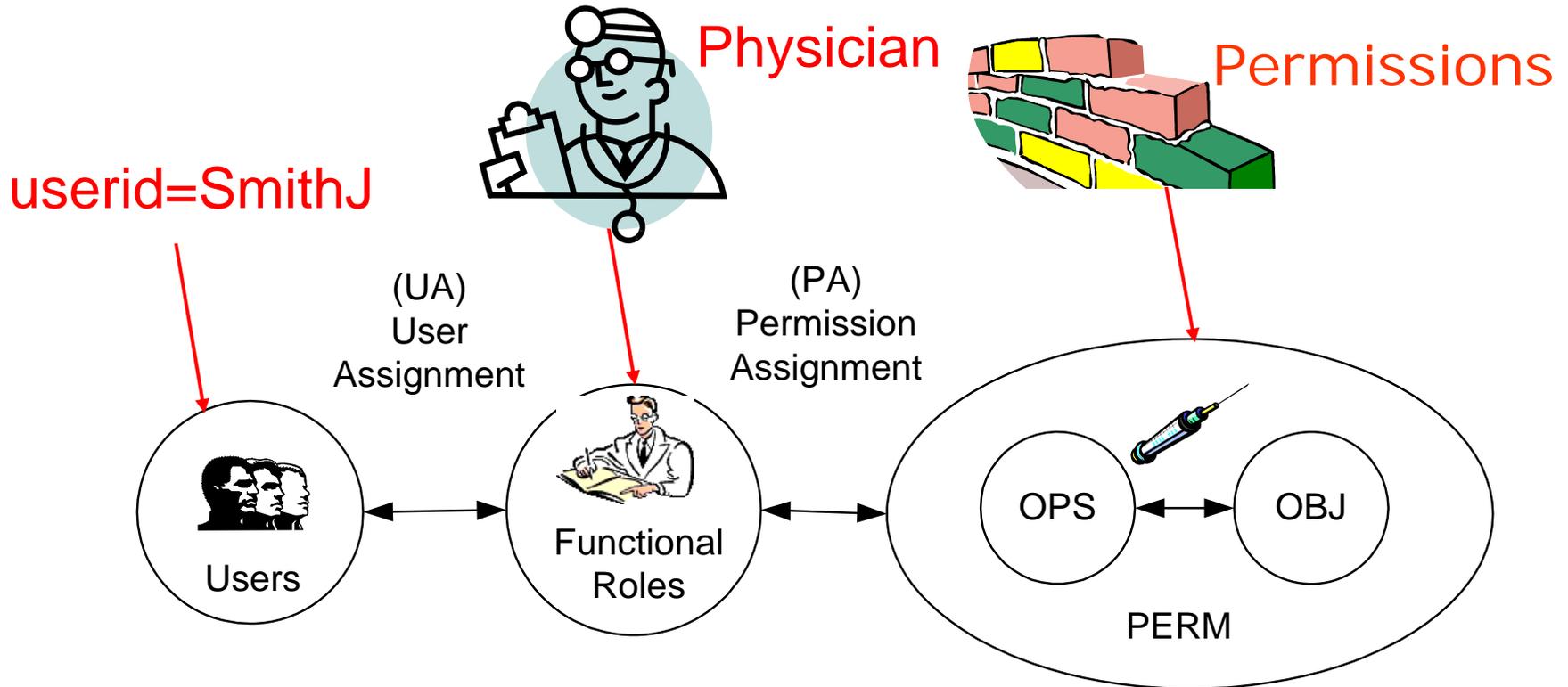


Roles are Built from Permissions



Enterprises create roles from HL7 standard permissions.

Permissions



OPS = Operations
OBJ = Objects
PERM = Permissions

Adapted from ANSI
INCITS 359-2004

RBAC Role Engineering Process

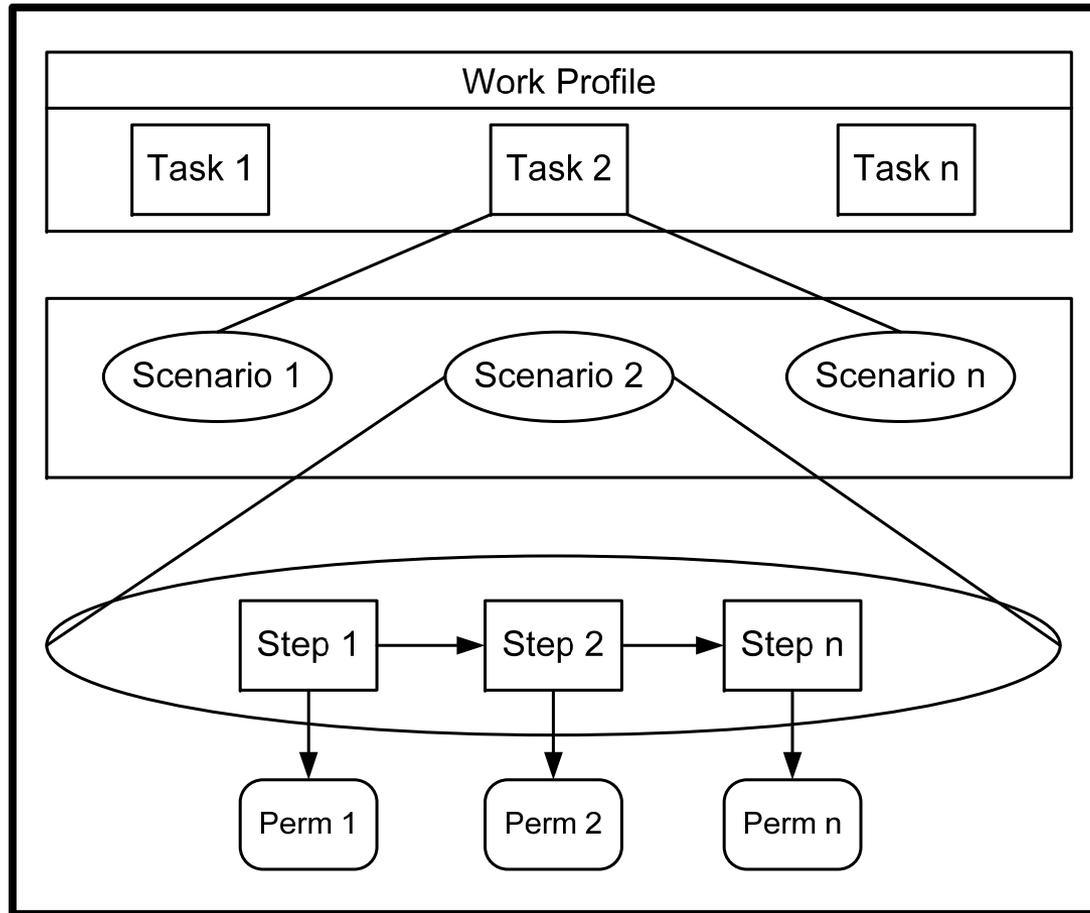
The VHA RBAC TF first developed a scenario-driven RBAC Role Engineering Process*, which is actively used by the VHA/IHS RBAC TF. The process has also been applied and proven within the Healthcare RBAC TF.

Role Engineering Process:

1. Identify and Model Usage Scenarios
2. Derive Permissions
3. Identify Permission Constraints
4. Refine Scenario Model
5. Define Tasks and Work Profiles
6. Define RBAC Model

*Adapted from *A Scenario-driven Role Engineering Process for Functional RBAC Roles*, G. Neumann and M. Strembeck. June 2002.

Scenario Model*



*Adapted from *A Scenario-driven Role Engineering Process for Functional RBAC Roles*, G. Neumann and M. Strembeck. June 2002.

1. Identify & Model Scenarios

- Sensible system usages are identified and modeled in terms of scenarios.
 - STEP 1 ➡ Gather healthcare scenarios.
 - STEP 2 ➡ Create steps and a sequence diagram for each scenario.
 - STEP 3 ➡ Validate and complete scenarios with input from healthcare experts.
 - STEP 4 ➡ Record consolidated list of scenarios.

1. Identify & Model Scenarios

- Example

Dr. Eric Emergency, an emergency room physician, sees a 45-year old male patient Adam Everyman, for chest pains. Myocardial infarction is suspected and the patient is admitted.

Dr. Emergency inquires if the patient Adam Everyman has any allergies, conducts a history and physical and [documents his findings in the patient's chart].

To determine whether patient Adam Everyman has had a heart attack, Dr. Emergency [orders a CPK] to be collected immediately and then every 8 hours for the next 2 days. Dr. Emergency also [orders a STAT Chest X-Ray].

STEP

SCENARIO

STEP

STEP

2. Derive Permissions from Scenarios

- For each scenario, the steps are identified and stored in the permission catalog as {operation, object} pairs.
STEP 1 ➔ Identify operations.
STEP 2 ➔ Find the associated object.
STEP 3 ➔ For each scenario step, record the associated (operation, object) pair in the permission catalogue.

2. Permissions - Example

Step	Permission
Perform ADT Functions (Admit Patient)	{ C, Admission }
New Patient Allergy	{ C, Allergy }
New History and Physical	{ C, History and Physical }
New Progress Notes	{ C, Progress Note }
New Laboratory Order (STAT CPK Panel)	{ C, Laboratory Order }
New Laboratory Order (q8 CPK Panel)	{ C, Laboratory Order }
New Radiology Order (STAT CXR)	{ C, Radiology Order }

3. Identify Permission Constraints

- Constraints to be enforced on permissions are identified and made explicit.

Constraints are:

- Restrictions that are enforced upon access permissions (e.g. Head Nurse, Chief of Staff).
- Include separation of duties, time-dependency, mutual exclusivity, cardinality or location.
- Distinguish healthcare policies that limit access to sensitive data (e.g. HIV, mental health, adoption).

4. Refine Scenario Model

STEP 1 ➡ The scenario is reviewed to see if some similar scenarios exist.

STEP 2 ➡ Similar scenarios are defined.

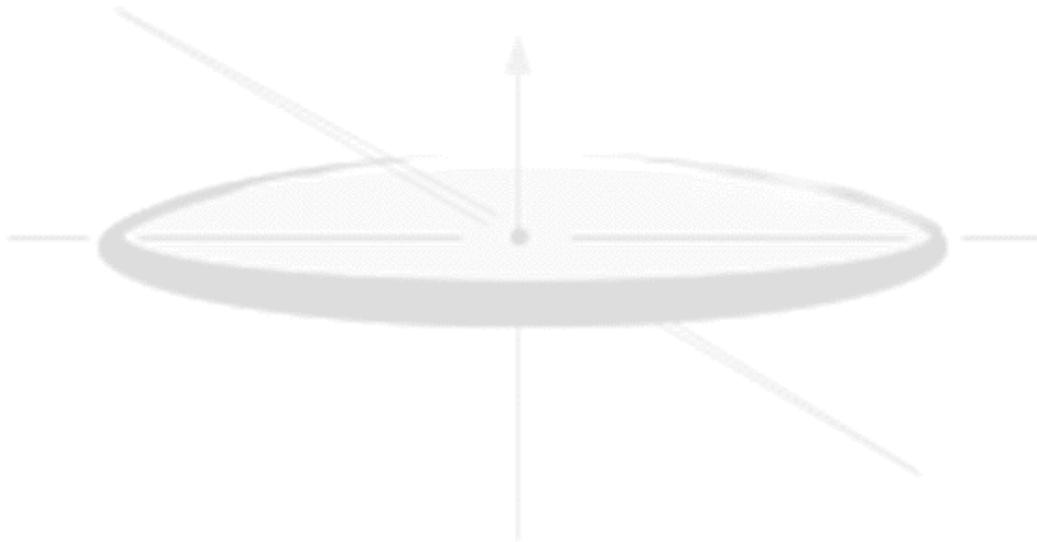
STEP 3 ➡ For each group of similar scenarios, determine if an abstract scenario can be defined.

STEP 4 ➡ The scenarios are grouped and a common abstract scenario is derived.

5. Define Tasks and Work Profiles

STEP 1 ➔ Identify scenarios that logically belonged together.

STEP 2 ➔ Group the scenarios into tasks.



6. Define RBAC Model

The role-hierarchy, permission catalog and constraint catalog define the RBAC model.

STEP 1 ➔ The work tasks and permission catalog are used to create a preliminary role-hierarchy.

STEP 2 ➔ Potentially redundant roles are identified and marked for review.

STEP 3 ➔ Redundant roles are removed, new roles and constraints are defined and role-hierarchies are merged or separated.

Summary

- We model scenarios, tasks and steps to understand people's jobs.
- We create access rules for each part of a job and call them permissions.
- We organize blocks of permissions and call them roles.
- We manage security and privacy for protected resources (like health information) with roles.
- We give people permissions (roles) they need to do their jobs (least privilege) and to access protected resources.
- We standardize permissions so we can share information among systems and partners.

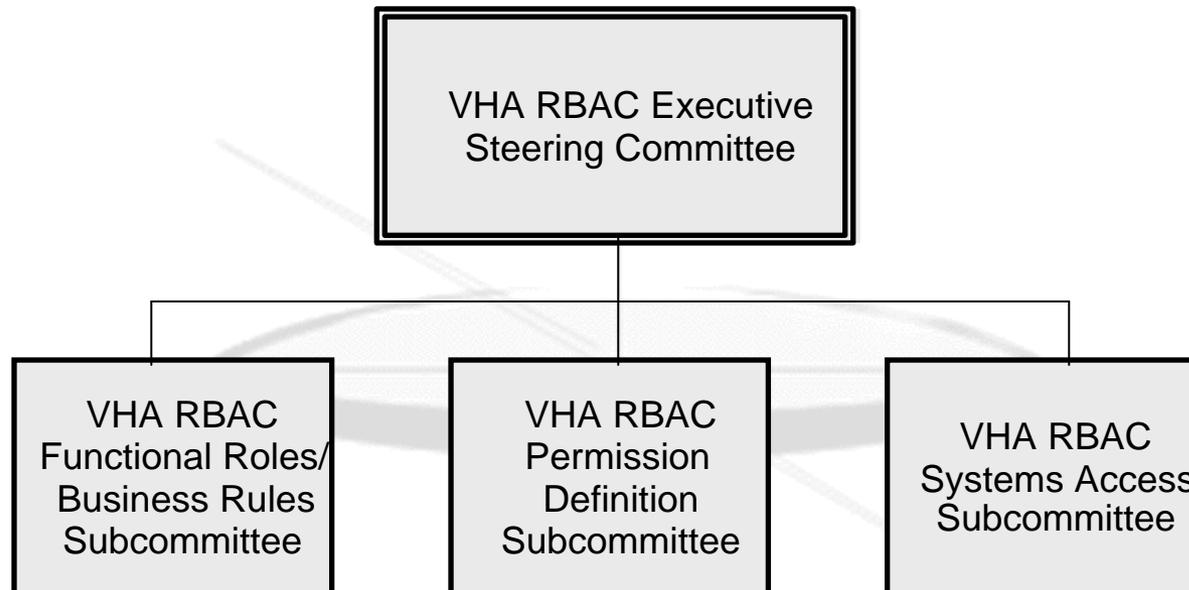
Next Steps

- Complete Healthcare Scenario Roadmap.
- Identify pilot project(s) to implement RBAC architecture in existing VistA and future HealtheVet-VistA systems.
- Perform Architectural Proof-of-Concept on XACML in VA lab.
- Map the permission catalog to VistA.
- Update AAIP architecture and requirements.
- Continue our involvement with SDOs and track the emerging standards.
- Engage interested international parties.

RBAC Workgroup



Proposed RBAC Organization



Proposed RBAC Organization

- **VHA RBAC Executive Steering Committee**
 - Coordinates overall direction of the RBAC effort
 - Harmonizes activities of VHA RBAC Subcommittees
 - Makes policy decisions across subcommittees
- **VHA RBAC Functional Roles/Business Rules Subcommittee**
 - Analyzes credentialing and privileging and how these dictate access to files
 - Role administration and provisioning
 - Break glass issues in emergencies
 - Issues regarding employees who are veterans
- **VHA RBAC Permission Definition Subcommittee**
 - Completes roadmap for licensed, non-licensed, and non-caregiver personnel
 - Writes and models scenarios down to the basic permission
 - Collector and trustee of VHA functional roles

Proposed RBAC Organization

- **VHA RBAC Systems Access Subcommittee**
 - Definition of RBAC architecture within VHA
 - Feeds architectural information to OCIS AAIP
 - Tracks NIST, ASTM and OASIS activities
 - Performs architectural proof-of-concepts to validate architectural risks
 - Develops interim RBAC solutions
 - Tracks development of OCIS AAIP
 - Maps permissions to VistA security keys and options
 - Integration with VistA and CPRS
 - Guidance for rehosted applications
 - Integration with AAIP Security servers
 - Tracks ISO activities
 - Resolves interoperability issues

RBAC Workgroup Charter

- Chuck Brown, Program Manager
- Charged with defining the scope of work involved with establishing these controls within existing VistA and future HealtheVet-VistA systems
- Includes staff from OI and field representation
- Reports to the Acting Chief Health Informatics Officer (Acting CHIO)

Workgroup Composition

- The RBAC Workgroup will include:
 - VHA Chief Architect
 - Deputy Director for HSD&D
 - Enterprise Systems Manager for Health Data Systems
 - Health_eVet VistA Project/Program Manager (chair)
 - 2 VISN CIOs
 - 2 field IRM Chiefs
 - Director Health Data and Informatics or designee
 - Technical Security Advisor for OI
 - Health Enterprise Strategy Representative
 - Physician Leadership Representative
 - 2 security and clinical representatives

RBAC Workgroup Tasks

- Identify all expectations related to Health_eVet VistA RBAC.
- Identify all efforts related to Health_eVet VistA RBAC.
- Document the current state of the VistA RBAC model and the to-be Health_eVet VistA RBAC model.
- Determine selection criteria for Project Manager.
- Develop project task matrix to define OI overlap and workflow.
- Develop a FAQs that will explain how RBAC will deal with everyday access issues.
- Develop management level presentation suitable for OI, IDMC, VA CIO, VISN Chief Information Officer Council (VCIOC), and Clinical leadership.

Information Resources

RBAC TF Team

- The VHA/IHS RBAC Task Force (TF) consists of clinical informaticists, software security architects, developers and managers from VHA and Indian Health Service (IHS).
- Members include:

Robert O'Hara, MD

Clayton Curtis, MD, PhD

CAPT Timothy Mayhew, MD

Hank Rappaport, MD

Rob Silverman, PharmD

Sharon Coleman, RN

Dawn Rota, RN

Geri Wittenberg, RN

Chuck Brown

Ed Coyne, PhD

Mike Davis

Beth Franchi

Gail Graham

Amy Page

Joel Russell

Steve Wagner

Nancy Wilck

RBAC Standards

OASIS  <http://www.oasis-open.org>

- eXtensible Access Control Markup Language (XACML), OASIS Standard 1.0
- LDAP Profile for Distribution of XACML Policies, OASIS Working Draft
- XACML Profile for Role Based Access Control, OASIS Committee Draft 0.1
- Service Provisioning Markup Language (SPML), OASIS Standard 1.0
- UDDI Version 2, 19 July 2002
- Web Services Security v 1.0, March 2004

NIST
National Institute of
Standards and Technology

<http://csrc.nist.gov/rbac>

- ANSI INCITS 359-2004



<http://www.astm.org>

- Healthcare Authorization Framework (E31 Committee Work Project)



<http://www.hl7.org>

- HL7 Healthcare Standard Permission Catalog (Security TC Work Project)

VHA

HEALTH INFORMATION

ARCHITECTURE

RBAC TF

42

Contact Information

- Website

<http://www.va.gov/RBAC/>

- Points-of-Contact

Robert O'Hara, MD
VHA/IHS RBAC TF Chair
Robert.OHara@med.va.gov
(708) 202-8387 x22759

Mike Davis, CISSP
VHA Security Architect
Mike.Davis@med.va.gov
(760) 632-0294

Amy Page
VHA/IHS RBAC TF
Project Lead
Amy.Page@med.va.gov
(619) 741-7587

Dawn Rota, RN, BSN
VHA/IHS RBAC TF
Functional Analyst Lead
Dawn.Rota@med.va.gov
(858) 826-7496

Q & A

Questions?

