

# **VHA Enterprise Role-Based Access Control Task Force Charter**

**Version 1.1**



June 19, 2003

VHA Enterprise RBAC Task Force Charter  
June 16, 2003

**TABLE OF CONTENTS**

<b>1</b>	<b>Scope.....</b>	<b>3</b>
1.1	Business Case.....	3
1.2	Objectives.....	3
1.3	Customer Needs.....	4
1.4	Work Products.....	5
1.5	Customer Requirements.....	5
1.6	Exit Criteria.....	5
1.7	Scope Boundaries.....	6
<b>2</b>	<b>Assurance.....</b>	<b>6</b>
2.1	Scope Risk Limit.....	6
2.2	Reviews and Approvals.....	7
2.3	Communications.....	7
<b>3</b>	<b>Resource Limits.....</b>	<b>8</b>
3.1	Team composition.....	8
3.2	Deadline.....	8
3.3	Task Force Constraints.....	8

**LIST OF TABLES**

Table 1:	Work Products.....	5
Table 2:	Exit Criteria.....	6

## 1 Scope

This charter document creates the VHA Enterprise Role-Based Access Control (RBAC) Task Force (TF) and describes the proposed tasks and goals to be accomplished the TF. This RBAC effort is an approved sub-project of the VA Authentication and Authorization Infrastructure Project (AAIP) and funding for the RBAC effort has been approved by AAIP.

It is expected that a number of enterprise RBAC task forces will be established in addition to the VHA RBAC TF. The VHA Enterprise RBAC TF will coordinate its efforts with the Healthcare RBAC TF, which is intended to be an oversight group for all the enterprise RBAC task forces. The Healthcare RBAC TF will be established initially with representatives from each of the large healthcare organizations participating in the RBAC effort, including Department of Defense (DoD), Indian Health Service (IHS), Kaiser Permanente (KP) and Department of Veterans Affairs (VA). Other healthcare organizations may join the collaboration in the future. Additionally, Standards Development Organizations (SDOs) will participate as advisory members.

The primary goal of the Healthcare RBAC TF is to define a common, industry-wide harmonized list of healthcare work profiles and access control permissions and present them as a recommended standard to a Standards Development Organization (SDO). Targeted SDOs include Health Level Seven (HL7), the American Society for Testing and Materials (ASTM) and the National Institute of Standards and Technology (NIST). The SDO would then turn the information into a proposed RBAC standard for use within the healthcare community.

### 1.1 Business Case

*"Should this person (or a person who performs this job function) typically be allowed to access this type of data?"*

RBAC is critically important to the security aspects of healthcare organizations. The Healthcare RBAC TF goal is to establish a mechanism for scalable management of user permissions in the form of a list of roles and tasks (role-based access), then provide that list to system access control and authorization services. The National Institute of Standards and Technology (NIST) defines role-based access as when: "access decisions are based on the roles that individual users have as part of an organization. Users take on assigned roles (such as doctor, nurse, teller, manager). The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization."

### 1.2 Objectives

In support of the Healthcare RBAC TF, the objectives of the VHA Enterprise RBAC TF are outlined below:

- Establish a VHA Enterprise RBAC TF composed of individuals who are knowledgeable in healthcare workflow and who will define tasks and permissions as a precursor to the development of an American National Standards Institute (ANSI) health information role

VHA Enterprise RBAC Task Force Charter  
June 16, 2003

standard. The VHA Enterprise RBAC TF will be composed of clinicians and personnel from within the organization's enterprise.

- Adopt the RBAC Role Engineering Process document, which includes standard terms, definitions and an RBAC process. Additionally, adopt both the *Proposed NIST Standard for Role-Based Access Control* document and the *A Scenario-driven Role Engineering Process for Functional RBAC Roles* article by G. Neumann and M. Strembeck as advisory materials.
- Identify and model usage scenarios from HL7 storyboards and other business system access patterns. Additionally, Enterprise participants and functionality experts will identify and define healthcare scenarios when other storyboards do not exist.
- Capitalize on enterprise-level projects to harmonize healthcare roles within the VA and DoD. VA-DoD collaboration is already established through Federal Health Information Exchange (FHIE), Clinical Data Repository-Health Data Repository (CHDR) and DoD/VHA interagency architecture and data sharing.
- Prepare and coordinate defined tasks, permissions and operations for healthcare roles, coordinating results through the Healthcare RBAC TF, to be used by an SDO for preparation of a draft healthcare RBAC standard.

### **1.3 Customer Needs**

RBAC was developed to overcome the complexities of managing individual user permissions. The Healthcare and Enterprise RBAC efforts are also motivated by the desires to:

- Simplify authorization management,
- Reduce administrative costs,
- Improve security,
- Enhance partner interoperability,
- Enable new network-level RBAC services, and
- Improve service to members/clients/patients.

The healthcare community and standards groups recognize RBAC as a high priority for numerous reasons, including:

- HIPAA privacy regulations (confidentiality of electronic patient records),
- National access and control standards,
- Interoperability,
- Data security, and
- System security.

Healthcare enterprises have a vested interest, clinically and financially, to ensure that RBAC needs, roles and definitions are adequately identified and resolved. Ultimately, results of the

VHA Enterprise RBAC Task Force Charter  
June 16, 2003

work of the Task Forces could establish and influence definitions of industry standards for RBAC permission management for use within the entire healthcare community.

### **1.4 Work Products**

The following table lists the Work Products to be prepared by the VHA Enterprise RBAC TF.

**Table 1: Work Products**

<b>Work Product</b>	<b>Description</b>
<b>Enterprise RBAC Task Force Plan</b>	This document will outline the management, activities, communications and risks.
<b>Healthcare RBAC TF Task List</b>	This work product is a list of tasks, permissions and operations for healthcare roles, coordinated by the Healthcare RBAC TF, to be used by an SDO for preparation of a draft healthcare RBAC standard. The task list may be in the form of a database export file.

### **1.5 Customer Requirements**

The high-level requirements that the VHA Enterprise RBAC TF shall satisfy include:

- The TF shall be a collaborative unit of the Healthcare RBAC TF.
- The TF shall use the RBAC Role Engineering Process to produce a list of tasks, permissions and operations for healthcare roles in the form of a permission catalogue, definition of tasks and work profiles, and a derivation of preliminary role hierarchies that can be used as input to a healthcare RBAC standard.

### **1.6 Exit Criteria**

The exit criteria are guideposts to indicate when the task forces have met goals in a satisfactory manner. Since this is a collaborative effort, the collaboration will need to collectively evaluate the adequacy of satisfying the defined exit criteria.

The following table provides the exit criteria with respect to the final deliverable, i.e., the Healthcare RBAC Task List.

VHA Enterprise RBAC Task Force Charter  
June 16, 2003

**Table 2: Exit Criteria**

<b>Exit Criterion</b>	<b>Description</b>
Completeness	<ul style="list-style-type: none"><li>• Does the goal or work product cover all recognized topics?</li><li>• Are these topics covered adequately?</li></ul>
Correctness	<ul style="list-style-type: none"><li>• Are all parts of the goal or work product free from significant errors?</li></ul>
Internal Consistency	<ul style="list-style-type: none"><li>• Are all parts of the goal or work product consistent with each other?</li></ul>
External Consistency	<ul style="list-style-type: none"><li>• Are all parts of the goal or work product consistent with other accepted sources?</li></ul>
Generality	<ul style="list-style-type: none"><li>• Is the goal or work product free of ad hoc assumptions and locally defined components?</li></ul>
Simplicity	<ul style="list-style-type: none"><li>• Are the parts of the goal or work product free of complex language or analysis that may impede the document's use?</li></ul>

### **1.7 Scope Boundaries**

The goal of the VHA Enterprise RBAC TF will be completed when a list of tasks and associated permissions are defined. HL7 and other storyboards and healthcare domain experts will provide the business workflows. The creation of a healthcare RBAC standard is not within the scope of these activities, but will be developed by the SDO committees.

The definition of roles is not within the scope of the VHA Enterprise RBAC TF. From an interoperability perspective, roles are irrelevant as they are configurable by organization and therefore, are not interoperable at the inter-organizational level. The list of tasks satisfies the interoperability requirements. The VHA Enterprise TF may, at its discretion, develop a suggested role set.

## **2 Assurance**

### **2.1 Scope Risk Limit**

If all of the exit criteria are not sufficiently met, the VHA Enterprise RBAC TF will have produced a less than optimum result that will affect the outcome of the Healthcare RBAC TF. In this case, additional work may be deemed necessary before RBAC can be successfully deployed within the enterprise. Because of the collaborative nature of the activities, the interoperability of the RBAC deployment across organizations may be similarly affected.

This collaborative aspect is itself a risk factor to the success of the Healthcare RBAC TF. Another risk factor will be the level of resources that can be made available for the VHA Enterprise RBAC TF activities. Therefore, it will be necessary to assess the accomplishment of the exit criteria on a continual basis. A mid-work product review should be planned to assess the likely outcome of the task force.

## **2.2 Reviews and Approvals**

Management review and approval will occur for the VHA Enterprise RBAC Task Force Charter and the VHA Enterprise RBAC Task Force Plan.

Collaboration review will occur for this charter document, the VHA Enterprise RBAC Task Force Plan, the RBAC Task Force Role Engineering Process document, and the Healthcare RBAC Task List.

## **2.3 Communications**

Communications will include formal and informal methods including e-mail, scheduled conference calls, status reports and potential face-to-face meetings.

**E-mail.** E-mail is used, as needed, for communication between VHA Enterprise RBAC TF members. Email will not be used to transmit sensitive data.

**Groove.** The Groove collaboration tool allows users to create secure interactive shared spaces where information, people and tools are all brought together seamlessly. Shared spaces sit on each user's PC. Work done in the space by one 'member' is instantly seen by all members. Groove keeps all members' PCs updated with the latest changes. All Groove data is automatically encrypted, thus protecting privacy and intellectual property. A free version of the software is available at [Http://www.groove.net](http://www.groove.net). VHA users requiring more than the three spaces permitted by the evaluation copy may obtain a VA license for an additional fee.

**Conference Calls.** Conference calls are scheduled, as necessary, to achieve the goals of the VHA Enterprise RBAC TF. Since this organization involves personnel all over the nation, it is anticipated that conference calls will occur frequently.

**Status Reports.** Status reporting will be achieved through a bi-monthly VHA Enterprise RBAC TF conference call. All Task Force members are expected to attend. The Project Lead will present a summary of current statuses and progress to the assembled team members, address current issues, and answers any questions. An advanced e-mail posting will provide all documents necessary for review prior to the monthly conference call. Minutes of the call will be prepared and distributed to the VHA Enterprise RBAC TF collaboration.

**Website.** A VHA Enterprise RBAC TF website will be established and realized as the primary location for all data input, review, and approval. This website will be enabled with mechanisms to ensure proper data access and operations on that data.

## **3 Resource Limits**

### **3.1 Team composition**

**VHA Enterprise RBAC TF.** VHA will establish its own Enterprise RBAC TF composed of knowledgeable individuals (healthcare providers, system developers, security experts, etc.) from within the organization. Representatives from the VHA Enterprise RBAC TF will participate in the Healthcare RBAC TF.

The actual resource levels will be estimated in the VHA Enterprise RBAC Task Force Plan. Funding for the resources necessary to support and coordinate the VHA effort is provided through the AAI Project. Additional resources related to domain expertise and general healthcare provider input will be obtained on a voluntary basis and will be dependent on commitments made by the collaborating VHA organizations.

### **3.2 Deadline**

Refer to the VHA Enterprise RBAC TF Plan for a detailed schedule of activities. The overall plan calls for an initial 90-day effort concentrating on 2-3 healthcare domains. Adjustments will be made to the process as a result of lessons learned during the initial effort. Subsequent efforts of approximately 90 days each will be conducted until all significant healthcare domains have been covered.

### **3.3 Task Force Constraints**

The primary constraints on the TF activities will be schedule and resources. As mentioned in Section 2.1, progress will be continually monitored to mitigate the effects of resource constraints.