



## Inside this issue:

- ✍ HL7 - RBAC Ballot Update
- ✍ Emergency Access & Break Glass
- ✍ TEPR Meeting
- ✍ RBAC Taskforce – Meeting Update
- ✍ Upcoming Meetings

### VHA/IHS RBAC TF Chair

Robert O'Hara, MD  
[Robert.Ohara@med.va.gov](mailto:Robert.Ohara@med.va.gov)

### VHA Deputy Chief Architect

RBAC Project Manager  
Steve Wagner  
[Steve.Wagner@med.va.gov](mailto:Steve.Wagner@med.va.gov)

### VHA Security Architect

RBAC Architect  
Mike Davis, CISSP  
[Mike.Davis@med.va.gov](mailto:Mike.Davis@med.va.gov)

### VHA Security Architect

RBAC Architect  
Ed Coyne, PhD  
[Ed.Coyne@med.va.gov](mailto:Ed.Coyne@med.va.gov)

### RBAC Project Lead

Suzanne Webb  
[Suzanne.Gonzales-Webb@saic.com](mailto:Suzanne.Gonzales-Webb@saic.com)

## HEALTH LEVEL SEVEN (HL7) WORKING GROUP MEETING MAY 1-3, 2007; Cologne, Germany

### *Role Based Access Control – HL7 Ballot Update*

The decision was made to proceed with an HL7 Out-of-Cycle ballot. The Out-of-Cycle ballot is being held for the continued RBAC ballot (DSTU to Standard) reconciliation. Updates to the HL7 RBAC Permission Catalog include A = Append to the Action Table. Append was defined as a fundamental operation in an information system (IS) that results only in the addition of information to an object or subject already in existence. The entire content of the updated RBAC document has been posted and can be reviewed at:

<http://www.hl7.org/v3ballot/html/welcome/introduction/index.htm>

Click the above link, then use the navigation link on the left-hand side of the page 'Link to HL7 Version 3.0 July 2007 Out-of-Cycle Ballot Site' to find the RBAC Ballot material under the 'Foundation' document group in the 'Security' DSTU.

**Recap:** The January 2007 Working Group Meeting held in San Diego marked the approval from the Security Technical Committee to revise the current balloted RBAC DSTU which would separate 'permission' vocabulary into 'actions and objects' to allow for more flexibility in the international realm.

### **Emergency Access and 'Break Glass' Terminology**

Proposed security definitions for 'break glass' and 'emergency access' were originally introduced at the January 2007 Security Technical Meeting. The HL7 Security TC members agree that there is a necessity to establish common semantics for "emergency access" and "break glass" and discussion has been assigned as a future agenda item. The terms are over-loaded, and that leads to confusion. In either case, legitimate care-providers with appropriate need must be able to acquire access to a specific patient and their patient record. Bear in mind that there are situations where a user may be unable to use the system because of a locked account, forgotten userid, password or expired account; these cases are administrative in nature and in general should not be considered as part of the definition of the terms. The situations being considered are those wherein an authenticated user is unable to assert authorization, or in the more likely case where the user (a provider or support personnel) lacks sufficient authorization which properly authorized personnel need to be able to immediately delegate in an emergency access situation.



## Upcoming Meetings

- ✍ Sarbanes-Oxley Symposium  
23–24 August  
Rosemont, IL USA
- ✍ Computer Audit, Control and Security (CACS) Conference Schedule  
September 9-12, 2007  
Auckland, New Zealand
- ✍ Information Security Management Conference  
September 10-12, 2007  
Las Vegas, NV
- ✍ International HL7 Interoperability Conference IHIC  
Aug 31 - Sept 1, 2007  
Auckland, New Zealand
- ✍ 21st Plenary & Working Group Meeting  
September 16 - 21, 2007  
Atlanta, GA

## RBAC Newsletter

ATTN: Suzanne Webb  
RBAC Project Lead  
10260 Campus Point MS-B1E  
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov



It remains to be said that in either definition, the access needed is for patient care and safety.

The Veterans Administration describes the two terms “break glass” and access to information *needed but normally not accessible* as part of day- to-day need-to-know workflow. The system should document (audit) any actual access for later review. Break glass access may or may not involve harm or risk to life. Within the VHA, users are presented with an application warning notice that is seen by the user as:

*‘You are entering a protected area. Your continued access of this area is your acknowledgement that this access is required for patient safety and care. You will be subject to additional monitoring and reporting of your activities’*

In the declaration of an ‘*emergency*’ specific pre-authorized individuals gain access to records containing protected health information when timely access is needed to prevent harm or risk to life. Emergency access as defined by the VHA would then include situations for which a caregiver would not normally have need-to-know access to a record, or where parts of a record or system functions allowed by ‘least privilege’ restrictions require an increased definitive and/or immediate delegation. Persons declaring an emergency must be properly authenticated and audited. Anonymous access to protected health information is not allowed.<sup>1</sup>

On the agenda in HL7’s May 2007 working group meeting was a continuation of the discussion for the common semantics for “emergency access” and “break glass,” again recognizing that the two terms are over-loaded leading to confusion. The HL7 Security Task Force is choosing “emergency access” as the term in the following use cases where in the pre-conditions of each case includes the need to access data for treatment and where an urgent patient safety issue exists.

Use case: Intra-domain emergency access

### ○ Pre-conditions:

- ✍ User’s security-mediated access permissions would normally allow access.
- ✍ Permission not granted by application system due to privacy policy restriction with a low assurance level (i.e., not assured per any security policies).

<sup>1</sup> VHA Personal Identity Verification Project (PIV) Requirements: Addendum 3, ‘VHA Emergency Access’ Version 2.1, Chief Health Informatics Office. February 26, 2007



## Upcoming Meetings

- ✍ **Third International Conference on Security and Privacy for Communication Networks**  
September 17th-21st  
Nice, France
- ✍ **INCITS Meetings**  
September 10-14, 2007  
Location: TBD
- ✍ **Sarbanes-Oxley Symposium**  
September 27-28, 2007  
Washington DC, USA
- ✍ **CCS'07 : 14th ACM Conference on Computer and Communications Security 2007**  
Oct 29 - Nov 2, 2007  
Alexandria, VA

## RBAC Newsletter

ATTN: Suzanne Webb  
RBAC Project Lead  
10260 Campus Point MS-B1E  
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov



- Post-conditions:
  - ✍ Access is granted according to security-mediated access permissions only.
  - ✍ An audit record is generated for privacy-policy override.

Use case: Extra-domain emergency access

- Pre-conditions:
  - ✍ Security-mediated access policies are not sufficient to allow the user's access.
  - ✍ High assurance is required to grant access (i.e., must be granted in accordance with security policies).
- Post-conditions:
  - ✍ Access is granted according to specific security policies for emergency access. In an RBAC security environment, this may be specific emergency-access permissions. "Emergency access permissions" may be subject to normative definition.
  - ✍ An audit record is generated for use of specific security policies for emergency access.

In continuing with discussion, the term "Emergency Room" was not considered an emergency access use case; it is a *normal* workflow scenario -- a general workflow container for a variety of access control policies.

Provisioning of users with identities and permissions is not an emergency access use case; it is a *normal* workflow scenario. Failure to do so in a timely manner does not create an emergency.

Not considered an emergency access use case was the failure to remember passwords or other lack of authentication. In this scenario, the case is considered part of a *normal* workflow scenario.

Also not considered an emergency access use case was a catastrophic event. The provision of care may require suspension of security controls as a matter of institutional policy, meaning to suspend security controls is not in this committee's scope.



## TEPR Meeting

An introduction to RBAC was presented at the TEPR (Towards Electronic Patient Record) Conference held in Dallas, Texas, May 18-23, 2007. The presentation highlighted work in progress between VHA and HL7 in covering key processes and techniques developed and being used toward the implementation of RBAC including the role engineering process, highlighting healthcare permissions and scenarios, constraints and relationships and describing the steps that organizations can take today to prepare for implementing their user roles and access control requirements.. A copy of the presentation will be posted on the RBAC Website shortly.

## RBAC Taskforce – Meeting Update

The RBAC Taskforce meeting calls are held on the **SECOND** Wednesday of every month at 1300CT / 1100PST / 1200MT / 1400EST; a meeting reminder is sent to current participants. If you would like to participate in the Task Force please contact Suzanne Gonzales-Webb for more information.

The RBAC Taskforce will continue discussions surrounding the definition of constraints on the current Permission Catalog and Roles, application of emergency access to the roadmap, as well as an update on RBAC incorporation into the VA re-engineering projects. Current Task Force Members are contacted with additional materials in preparation for the meeting.

~

Role-Based Access Control is critically important to the security aspects of the VA and other healthcare organizations. There is a growing management and security demand for RBAC to be implemented in healthcare systems.

RBAC grants rights and permissions to roles rather than individual users. Users then acquire the rights and permissions by being assigned to appropriate roles. By grouping individuals with other individuals who have similar access rights, RBAC can provide significant security management efficiencies.

The latest RBAC Documentation additions and prior RBAC Newsletters can be found on the RBAC Website.

~

**The RBAC Newsletter is now published quarterly instead of monthly. Please be on the lookout for the next issue due October 2007!**

## RBAC Newsletter

ATTN: Suzanne Webb  
RBAC Project Lead  
10260 Campus Point MS-B1E  
La Jolla, CA 92121

Or e-mail:

[Suzanne.Gonzales-Webb@va.gov](mailto:Suzanne.Gonzales-Webb@va.gov)

~