



## Inside this issue:

- ✍ RBAC DSTU Update
- ✍ HL7 Ballot Notes
- ✍ RBAC Taskforce – Meeting Update
- ✍ Upcoming Meetings

## HEALTH LEVEL SEVEN (HL7) WORKING GROUP MEETING - JANUARY 8-12, 2007 San Diego Town and Country Resort, San Diego, California

### Draft Standard for Trial Use (DSTU) Ballot Update

**Recap:** January 2006 marked the submission of the Role Based Access Control (RBAC) Permission Catalog for use at HL7 as an International Standard. This submission was voted upon and passed by the members of the technical committees within this standards organization. As one of only two affirmative ballots approved during the HL7 January 2006 ballot cycle, the RBAC DSTU provides healthcare organizations an ANSI (American National Standards Institute) compliant permission catalog needed to evaluate enterprise-wide RBAC.

**Update:** The January 2007 Working Group Meeting held in San Diego marked the approval from the Security Technical Committee (TC) to revise the current balloted RBAC DSTU that separates ‘permission’ vocabulary into ‘actions and objects’ to allow for more flexibility in the international realm. It was noted in the same meeting that the lack of implementation of current RBAC DSTU is problematic, but was not viewed as discouraging the forward progression of the revised ballot information, but allowed for more flexibility and wider acceptance from the international community.

Introduced at the Security Technical Meeting were proposed security definitions for ‘break glass’ and ‘emergency access.’ The terms are over-loaded, and that leads to confusion. 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. Legitimate care-providers with appropriate need must be able to acquire access to a specific patient and their patient record. Keeping 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. It is more likely that 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 (in other words, when an authenticated user is unable to assert authorization). It remains to be said that in either definition, the access needed is for the patient care and safety.

The Veterans Administration describes the two terms “break glass” and “emergency access” as: “Break the Glass” allows caregivers access to information needed but normally not accessible as part of day-

#### 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)

#### VHA Security Analyst

Sepideh Khosravifar  
[Sepideh.Khosravifar@va.gov](mailto:Sepideh.Khosravifar@va.gov)

#### RBAC Project Lead

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



## Upcoming Meetings

- ✂ **4th ACM Conference on Computer & Communications Security**  
April 1-4  
Zurich, Switzerland
- ✂ **INCITS Meetings**  
April 10-12, 2007  
Redmond, WA
- ✂ **6th Annual Security Conference**  
April 11-12, 2007  
Las Vegas, NV  
<http://www.security-conference.org/>
- ✂ **OASIS Symposium: eBusiness and Open Standards**  
April 15-20, 2007  
San Diego, CA
- ✂ **HL7 May Working Group Meeting**  
April 29-May 4, 2007  
Cologne, Germany
- ✂ **SACMAT '01: 6th ACM Symposium on Access Control Models and Technologies (formerly known as RBAC)**  
May 3-4, 2007  
Chantilly, VA
- ✂ **Web Services Security Conference & Exhibition**  
May 8-9, 2007  
Baltimore, MD

to-day need-to-know. The system should document (audit) any actual access for later review. Break the glass may or may not involve harm or risk to life. Typically, the user is presented with an application warning notice that says something to the effect: *'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 includes situations for which a caregiver would not normally have need-to-know access to a record, or parts of a record or system functions covered by *'least privilege'* restrictions which require definitive, immediate delegation. Persons declaring an emergency must be properly authenticated and audited. Anonymous access to protected health information is not allowed.<sup>1</sup>

As a standards development organization, HL7's mission is to provide standards for the exchange, management and integration of data that support clinical patient care and the management and delivery of healthcare services by defining the protocol for exchanging clinical data between diverse healthcare information systems. The HL7 organization works through volunteer efforts to create flexible, cost-effective approaches, standards, guidelines, methodologies and related services for interoperability between healthcare information systems.

## HL7 Balloting Notes:

March 4 (Sunday) T minus 2

All Submissions: Reconciliation, Complete & Supporting Content Deadlines will have been completed. All previous ballot reconciliations must be completed and appropriately captured on the ballot website. The deadline for the required documentation is the Supporting Content Deadline, scheduled two weeks prior to ballot opening. For the May 2007 Ballot, this deadline is March 4. In the coming weeks, a document from HQ that lists the outstanding items by ballot cycle will be provided to the TSC list.

March 11 dates the Final Content Deadline, where only changes expressly requested by the technical publishers will be made to content after this deadline.

---

<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

- ✍ **2007 IEEE Symposium on Security and Privacy**  
May 20-23, 2007  
Berkeley/Oakland, CA
- ✍ **SACMAT '03: 8th ACM Symposium on Access Control Models and Technologies 2003**  
June 1-4, 2007  
Como, Italy
- ✍ **SACMAT '02: 7th ACM Symposium on Access Control Models and Technologies**  
June 3-4, 2007  
Monterey, CA
- ✍ **Computer Security Institute (CSI) NetSec '07**  
June 11-13, 2007  
Scottsdale, AZ
- ✍ **12th ACM SACMAT**  
June 20-22, 2007  
Sophia Antipolis, France
- ✍ **INCITS Meeting**  
July 18-20, 2007  
Location TBD

## 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)

~

March 19

Ballot Opening – This is the earliest date that the ballot site can open and be announced to the membership. In any event, the ballot must open before the end of this week.

## RBAC Taskforce – Meeting Update

The RBAC Taskforce meeting calls are held on the first 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 will now be published quarterly instead of monthly.  
Please be on the lookout for the next issue due July 2007!**