Help in Setting Access Controls: Using the HL7 RBAC Healthcare Permission Catalog to Reduce Data Breaches

by Margret Amatayakul, MBA, RHIA, CHPS, CPEHR, FHIMSS

Healthcare providers are looking for ways to reduce the risk of data breaches; however, tighter access controls that would help thwart inappropriate internal access to protected health information have been challenging to implement. Health Level Seven's RBAC Healthcare Permission Catalog, published in November 2007, can make the task easier and ensure interoperability across applications.

Tracking Data Breaches

The Identity Theft Resource Center tracked 342 data breach reports in the first nine months of 2008.[1] Lost or stolen laptops and other digital storage media were the most frequent cause of reported breaches (20 percent), followed by insider theft (17 percent). Inadvertent posting of information online accounted for 14 percent of reported breaches, and hacking was the cause of 13 percent. However, it is difficult to collect and analyze data because breaches are reported inconsistently.

In another study, Verizon suggests a shift from internal to external threats—although external attacks are more likely to occur from a privileged business partner, and insider breaches have consequences greater than external breaches by tenfold.[2]

Need for Tighter Technical Controls

Tighter technical controls that reduce the risk of internal data breaches is one important step. Adoption of role-based access controls (RBAC) marries the HIPAA privacy rule's minimum necessary standard with the security rule's information access management and access controls requirements.

RBAC enables access permissions to focus on a predefined set of operations that may be performed on given objects by persons or systems authorized to perform such operations (i.e., the person's role or job function within the context of specific authority and responsibility). The table "RBAC Permissions" below outlines how RBAC assign permissions according to role or function.

RBAC technology was developed by the InterNational Committee for Information Technology Standards (INCITS) and approved as an American National Standards Institute (ANSI) in 2004. ANSI INCITS 359-2004 provides a reference model that defines basic RBAC elements—users, roles, permissions, operations, and objects—and their relationships. It also provides the RBAC System and Administrative Functional Specification that describes the features required of a RBAC system.[3]

The RBAC Healthcare Permission Catalog

In 2007 Health Level Seven (HL7), an organization that develops standards for the exchange, integration, sharing, and retrieval of electronic health information, developed the RBAC Healthcare Permission Catalog, which conforms to ANSI INCITS 359-2004 for the healthcare domain. The combination of these two works enables health information systems vendors to implement RBAC technology in their products, providing a mechanism for scalable management of user permissions that provides information accessibility on a need-to-know basis and promoting interoperability across products.

The catalog provides a vocabulary defining pairs of operations and objects for permission representation. It contains 56 objects for everything from accounts receivable to vital signs and patient measurements. The table "Sample Healthcare Permissions Catalog Objects" below offers a sample of objects contained in the catalog.

When objects are combined with one of the five basic operations—create, read, update, delete, and execute—the operation-object pair can be assigned a given permission. The result is a large set of potential permissions, such as "create new diet order" or "change/discontinue nursing order." HL7 includes examples of healthcare permission tables in the catalog, including 26 permissions associated with order entry, 17 with reviewing documentation, 43 with performing documentation, five with scheduling, and 15 with administration.

RBAC Permissions

Role-based access control (RBAC) focuses access permissions on a predefined set of operations that may be performed on given objects by persons authorized according to their role or function. An object is a system resource subject to access control, such as a file, table in a database, printer, or CPU cycles. Operation is an executable image of a program which, once invoked, executes a function for a user.

	RBAC	**Example 1**	**Example 2**
Privacy Rule			
Minimum necessary requirements			
1. Identify persons or classes of persons who need access to protected health information to carry out their duties	Role	Physician	Dietitian
2. For each person or class of person, identify the category or categories of protected health information to which access is needed	Object 1	Diet order	Diet order
3. For each category or categories, identify any conditions appropriate to such access	Operation 2	Create	Read
Security Rule			
Access authorization	Permission (approval to perform an operation on an object)		
Implement policies and procedures for granting access	User	Dr. Smith is a physician	John Jones is dietitian
Access Controls			
Implement technical policies and procedures for electronic information systems to allow access only to those persons or	Implementation		

software programs that have been granted access rights			

Defining Different Roles

An organization may not need every type of permission, and it may assign different users to different roles or create unique combinations of roles (e.g., physician and coder). HL7 thus recommends use of a "role engineering" process to fully identify all users, roles, objects, operations, and permissions in a given organization. The Veterans Health Administration recommends the creation of a road map through which the organization identifies all healthcare tasks and links them to all personnel who may perform those tasks.[4] A sample of the road map is provided in the table below.

Sample Healthcare Permissions Catalog Objects

The HL7 RBAC Healthcare Permissions Catalog provides a vocabulary defining pairs of operations and objects for permission representation. It contains 56 objects for everything from accounts receivable to vital signs and patient measurements. Samples are shown here.

Object	Definition	Source of Definition
Advance directives	A living will written by the patient to the physician in case of incapacitation to give further instructions.	ASTM E1384-02a Standard Practice for Content and Structure of the Electronic Health Record
Coding	Coding is a process where medical records produced by the health care provider are translated into a code that identifies each diagnoses and procedure utilized in treating the patient.	Mississippi Hospital Association Health Career Center, www.mshealthcareers.com/careers/healthinfo.htm
Diet order	An order for a patient diet. A patient may have only one effective diet order at a time.	HL7 Version 2.3 1997 www2.dmi.columbia.edu/resoruces/hl7doc/hl72.3/APPE.PDF

VHA's Road Map for Healthcare Tasks

Because each organization is different, HL7 recommends "role engineering" to fully identify all users, roles, objects, operations, and permissions in a given organization. The Veterans Health Administration recommends creating a road map that links all healthcare tasks to the personnel who may perform them. The excerpt here serves as an illustration.

Permission ID	Scenario ID	C = Create R = Read U = Update D = Delete E = Execute Operation/ Object	X = Performs O = Does not perform Task	Acupuncturist	Audiologist	Coder	Dentist	Dietitian	Nurse Anesthetist	Nurse Specialist	Physician	ROI Specialist
POE-001	SOE-002	[C, Lab Order]	New Lab Order	O	O	O	X	O	X	X	X	O

Enhancing the Catalog

HL7 notes that the vocabulary in its catalog enables organizations to adopt a total and interoperable access management solution. By conforming to the definitions, there is no ambiguity across different applications. HL7 also recognizes that organizations may want to define new operation-object pairs, in which case HL7 urges organizations to submit proposed changes to HL7 for consideration in the development of the next version of the standard.

However, it is also possible to preserve the integrity of the standard and still add enhancements. For example, some organizations have added context factors (such as time or place) to their RBAC systems to further strengthen their gate-keeping functionality. A nurse may only be able to review chief complaint from a desktop or wireless access point within the proximity of the nursing unit where she is assigned. In this case, the RBAC policy conforms to the HL7 catalog, but the context constraints are added.

Many organizations express concern that detailed RBAC systems are difficult to administer. They note that roles change often, such as a nurse reassigned to another nursing unit or working a second shift in the emergency department. However, the catalog can accommodate multiple roles.

For example, it may be that every nurse is provided the ability to review chief complaint from any nursing unit, but only for patients on one nursing unit at a time. The system could generate a report of any time a nurse signs onto a workstation at any nursing unit other than the primary one assigned, and this can be compared with the nurse's work schedule. Furthermore, with "break-the-glass" functionality that enables access beyond the assigned role permission the result can be a strong deterrent to internal data breaches.

However an organization implements the permission catalog, it must be remembered that any technical security control is only as good as its management. Controls must be properly set up, used consistently, and actively followed up.

In 2007 the *Minneapolis Star Tribune* reported that a number of hospitals in Minnesota were cracking down on unauthorized employee access to electronic health records.[5] One facility that applied a "zero-tolerance" policy suspended more than 100 employees; most violations involved accessing a friend or relative's record. The crackdown stopped the activity.

Notes

1. Krebs, Brian. "Report: Data Breaches Expose about 30M Records in '08." *Washington Post,* October 6, 2008. Available online at http://voices.washingtonpost.com/securityfix/2008/10/516_data_breaches_in_2008_expo.html.
2. Verizon Business RISK Team. "2008 Data Breach Investigations Report." Available online at www.verizonbusiness.com/resources/security/databreachreport.pdf.
3. American National Standard for Information Technology and InterNational Committee for Information Technology Standards. Information Technology—Role Based Access Control (ANSI INCITS 359-2004). InterNational Committee for Information Technology Standards, 2004.

4. Gonzales-Webb, Suzanne. "Implementing Role Based Access Control (RBAC) in Healthcare." Veterans Health Administration. Presentation. Available online at www.va.gov/RBAC/documents.asp.
5. "Minnesota Facilities Target Unauthorized Employee EHR Access." *Minneapolis Star Tribune*, July 19, 2007.

References

Gelzer, Reed. "Developing Emergency Access Standards for EHR Systems: The HL7 Standards Development Process Helps (and Empowers) HIM Processes." *Journal of AHIMA* 79, no. 6 (June 2008): 52–53.

Health Level Seven. "Role Based Access Control (RBAC) Healthcare Permission Catalog, Version 3.38." November 2007. Available online at www.va.gov/RBAC/docs/Stds_20071129_SW_22_5_HL7_RBAC_Healthcare_Permission_Catalog_v3_38.pdf.

Wilikens, Marc, Simone Feriti, Alberto Sanna, andMarcelo Masera. "A Context-Related Authorization and Access Control Method Based on RBAC: A Case Study from the Health Care Domain." Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, June 2002, Monterey, CA.

Margret Amatayakul (Margret@margret-a.com) is president of Margret\A Consulting, LLC.

Article citation:
Amatayakul, Margret. "Help in Setting Access Controls: Using the HL7 RBAC Healthcare Permission Catalog to Reduce Data Breaches" *Journal of AHIMA* 79, no.11 (November 2008): 56-57;61.