Electronic health records (EHR) convey a set of health information on systems designed to assist healthcare practitioners. EHR systems hold records of various types including patient demographics, treatment behaviors and evolution, procedures performed, international classification of disease (ICD-10) diagnoses, laboratory tests, and other inputs. The required degree of health information and details needed to be registered may vary according to medical specialty or system purpose.

The patient is the sole owner of all this information; therefore, accessing it to deliver the required medical attention demands privacy boundaries to be established, defining who is allowed to see what EHR portion on the system. We must consider that the patient may be assisted by a number of professionals from different fields (nurses, physicians, surgeons, physical therapists, radiographers, radiotherapists, etc.). Also, the patient may not necessarily go to the same hospital or medical center, and hence the information is not only spread as chunks among various professionals’ specific interfaces and containers but also divided among different users in different devices (mobile device, other systems…) and locations.

Nowadays, part of a patient’s EHR can even be found on his mobile phone and health cards. Thus, the challenge of health information management is not only related to privacy limitations or access restrictions but also integrating the information as a whole for a more complete view. Personal health information (PHI) access is restricted and should be disclosed under specific conditions to healthcare practitioners as temporary information custodians. This includes not only patient treatment but also supporting healthcare management and planning through statistics for field researchers using anonymized/pseudonymized data for analysis, or even law enforcement official requests. Disclosure regulations and security requirements examples for that matter include the Personal Health Information Act (PHIA) from Canada [1], the US Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rule [2], the NHS-Data Protection Act from England [3], and the Brazilian Society of Health Informatics (SBIS) certification program in Brazil [4].

Access control plays an important role in information access restrictions with the above-described scenario—more technically speaking, authorization capabilities of applied access control on information systems. Authorization is the third phase in a generic access control, occurring after the identification and authentication processes. During authorization, the objects (information, system functions, etc.) are mapped to user permissions so they may be controlled. Authorization deploys security policy based on what the authenticated user is allowed to do on the system. Generally, it is performed by mapping existing objects and permissions in an access control matrix table. Depending on the implemented authorization of access control on an EHR system, security policies are applied differently. Formal options include mandatory access...
control, discretionary access control, and non-discretionary access control.

- **Mandatory access control** (MAC) refers to a centralized access decision model based on an object (target) label. Access controls implementing this model do not allow users to change the object settings or account security attributes.

- **Discretionary access control** (DAC) refers to the data-owner’s ability to transfer part or all of the available system authorization to other users. DAC implementations allow security policies to be initially dictated by an administrator and then assigned to users to propagate among other users accordingly (under owner discretion).

- **Non-discretionary access control** (NDAC) is another option of centralized administration and is based on roles or tasks related to users for access decisions. The most common example of NDAC on systems is role-based access control (RBAC). In this type of implementation, authorization is assigned to roles instead of users directly. Therefore, the roles can be seen as an authorization umbrella that suits or describes the permission needs of a healthcare professional or a specific employee position within the organization’s staff hierarchical structure reflected in that information system. In other words, RBAC addresses the needs for authorization control over objects, adding maintenance/administration features of grouping users that have the same permissions/needs into roles.

Currently, RBAC is globally the most commonly used access control model to cope with EHR requirements [5]. It’s been around for roughly 20 years, formalized in 1992 and published by the US National Institute of Standards and Technology (NIST) in 2000 [6]. It was added as a mandatory requirement in 2016 for certified EHR systems (EHRS) under Brazilian SBIS scope. Actually, in a recent Brazilian online survey designed to map current access control models in order to foresee next-generation EHRS implementation intentions in the Brazilian market (138 respondents,) we see this data confirming various RBAC models totaling nearly 40 percent of respondents, although in our scenario basic access-matrix-based implementations are still present (see table 1). Considering our questions asking for future implementation prediction (access control change in short-, medium-, or long-term planned implementation), DAC-MAC hybrid, RBAC full, and RBAC mixed extensions (time and context based) are what we should see for EHR systems in the near future.

<table>
<thead>
<tr>
<th>AC model</th>
<th>Current implementation</th>
<th>Currently satisfies industry needs</th>
<th>Planned implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;12m</td>
<td>&lt;36m</td>
<td>&gt;36m</td>
</tr>
<tr>
<td>AC matrix basic</td>
<td>14.2%</td>
<td>6.7%</td>
<td>1.5%</td>
</tr>
<tr>
<td>DAC</td>
<td>1.5%</td>
<td>1.5%</td>
<td>0</td>
</tr>
<tr>
<td>MAC</td>
<td>8.2%</td>
<td>6.0%</td>
<td>0</td>
</tr>
<tr>
<td>Hybrid (above)</td>
<td>8.2%</td>
<td>7.5%</td>
<td>1.5%</td>
</tr>
<tr>
<td>RBAC (Core)</td>
<td>16.4%</td>
<td>12.7%</td>
<td>0.7%</td>
</tr>
<tr>
<td>RBAC full</td>
<td>5.2%</td>
<td>5.2%</td>
<td>0.7%</td>
</tr>
<tr>
<td>RBAC time-based</td>
<td>15%</td>
<td>0.7%</td>
<td>0</td>
</tr>
<tr>
<td>RBAC context-based</td>
<td>3.0%</td>
<td>2.2%</td>
<td>0</td>
</tr>
<tr>
<td>RBAC mixed</td>
<td>13.4%</td>
<td>11.2%</td>
<td>3.0%</td>
</tr>
</tbody>
</table>

Table 1 – Survey responses considering current and planned access control implementation on Brazilian EHRS systems
Access Control Capabilities and Healthcare Informatics Needs

Healthcare routine access control demands

In a recent literature review exploring articles related to security and privacy trends for EHR, I’ve found different specific concerns related to the healthcare industry. To highlight severe impact challenges to the authorization process, example scenarios are described for discussion below.

Least privilege

Interconnected systems, healthcare treatment dynamics and multidisciplinary medical specialties related to professionals, and emergency situations all present varying access control demands imposed by healthcare routines. Considering the most common access control model—RBAC—one important healthcare security demand is the ability to promote least privilege best practices.

In this sense, RBAC roles may not have the ideal granularity for that purpose. The RBAC model comprises four major components: core, hierarchical, static separation of duty, and dynamic separation of duty relations. The core component represents basic access control features related to role creation and attribution to users. By using hierarchy, administrative tasks could be saved but least privilege may be compromised. That’s because managing permissions using this feature results in adding authorization that needs to be carefully applied. In figure 1, medical director, cardiologists, and rheumatologists share doctor and resident permission sets. Cardiologists and rheumatologists share specialists permissions. All three have their own permission sets. Users can be bound to many roles that have many permissions to EHR-system mapped objects. By receiving hierarchical authorization, a user’s resulting conjunction of roles may represent more than those necessary to perform specific duties, even considering that the individual roles applied in the chain were created using the minimal permission concept in mind while viewed separately.

The very nature of healthcare treatment is dynamic. It’s not easy to strictly define healthcare practitioner needs in terms of access to EHR systems information or functions because routines cannot always be predicted. The same user may have specific functional needs while working at a triage station but later a broader view while attending to emergency room tasks. Also, due to medical plurality in terms of specialties, a user may act as a clinical physician in the morning, therefore requiring diagnostic system features. But during the following shift the system interaction may be related to gastroenterology, therefore requiring a whole new set of system functions. This example shows how complex the achievement of least privilege using RBAC alone can be. Time-based or context-based RBAC extensions are proposed in the literature to address dynamic environments. These adaptations promote transient access-decisions to cope with occasional permissions needs on an EHR system. Actually, NIST is currently providing case studies to understand industry-specific needs. Examples of a working group related to the healthcare industry can be seen at NIST “Role Engineering and RBAC Standards [7], which includes the following: HL7 Security and Accountability SIG, VA RBAC and Role Engineering site, Healthcare Role-Based Access Control Task Force, HIPAA Security Requirements, HIPAA Advisory on RBAC, and HIPAA rules.

Emergency access and PHI disclosure

The Hippocratic Oath and the swearing of putting patient care above all other interest (or other ethics pledge) are commonly seen as medical students transition to doctors. Although this is more an idealistic process, and the “do no harm” has literally little or no impact on a doctor’s behavior in real life, patient priority is indeed what needs to be considered in any system access-control constraint. After all, these days a doctor will not be able to treat anyone without the need of systems interaction simply because clinics, smaller facilities, and hospitals—virtually all healthcare facilities—are driven by electronic authorizations.

In such cases, the EHR system needs a way to ensure authorization control so a patient can be treated. This feature can be seen in the literature as a “breaking the glass” emergency function. Advised emergency practices usually advocate two-step activation (different users) for this state to be declared (so collusion can be avoided) and include a tightened audit trail. That’s because this special condition needs to actually be an exception so authorization sets are not overruled simply to ease daily processes in terms of access constraint. Notice, though, that even during this phase the healthcare professional may face blocked access to patient data because the electronic health record has privacy locks that demand explicit authorization by its owner (the patient). RBAC has no native feature for that purpose, so common suggestions to solve the issue involve combining the discretionary function from DAC capabilities, treating the patient as a regular EHR user so that he could edit access control permissions over his own data objects. If patient is unresponsive, “breaking the glass” is enforced.
Warfare has advanced considerably since the Middle Ages, but in many ways the principles of fortification remain the same. The great castles of antiquity were ingeniously designed to protect their inhabitants from persistent enemy threats. Their carefully planned and creative defensive measures provide rich metaphors for today’s cyber guardians. SecureWorld attendees will enjoy exploring and learning from the historical anecdotes and tactics in this year’s conference theme.

Join like-minded security professionals in your local community for high-quality, affordable training and education. Attend featured keynotes, panel discussions and breakout sessions, and learn from nationally-recognized experts. Network with fellow practitioners, thought leaders, associations and solution vendors.

**Don’t go it alone. Register for a SecureWorld conference near you.**

www.secureworldexpo.com

Our Fall 2017 event schedule will kick off with the first annual Twin Cities conference. Mark your calendars and make plans to attend!

**Fall:**

<table>
<thead>
<tr>
<th>Location</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twin Cities, MN</td>
<td>Sept. 6</td>
</tr>
<tr>
<td>Detroit, MI</td>
<td>Sept. 13-14</td>
</tr>
<tr>
<td>St. Louis, MO</td>
<td>Sept. 20-21</td>
</tr>
<tr>
<td>Bay Area, CA</td>
<td>Oct. 5</td>
</tr>
<tr>
<td>Dallas, TX</td>
<td>Oct. 18-19</td>
</tr>
<tr>
<td>Cincinnati, OH</td>
<td>Oct. 24</td>
</tr>
<tr>
<td>Denver, CO</td>
<td>Nov. 1-2</td>
</tr>
<tr>
<td>Seattle, WA</td>
<td>Nov. 8-9</td>
</tr>
</tbody>
</table>
Interconnection of systems

Interconnected EHR systems represent another challenge in promoting access control. RBAC was not originally developed to cope with multiple security policies. That’s because the centralized access decision point (ADP) is not able to map the different users’ attributes and system objects that are not locally bound. The scenario is described as “cross-border” access control in the literature, where a few workarounds are proposed. ISO 22600, for instance, includes adding a neutral third-party (certification authority) PKI entity to issue mutually accepted (from both hospitals, for example) identification to users. The advised issuing procedure incorporates special tags (attribute certificates) to identify healthcare professional specialties and government issued IDs, broadly characterizing the users in a way both ADPs could differentiate and apply corresponding authorization restrictions.

The other workaround is a little trickier because local system objects are too particular to be standardized. Data dictionary (database collection of information descriptions) and system functions exemplify the particularity of objects that would be “controlled” by the outer EHRS. On top of that, we need to consider the information classifications deriving security policies that will be used to compose the ADP access-matrix, which are unique to each facility/organization. The challenge is more complex than the simple domain or forest of trust we see today in Active Directory trusted domain objects (TDO) [8], allowing authenticated users to connect to external realms and shared objects (depending on the trust direction configured) to translate local ADPs to cross borders accordingly.

Meaningful use and object identifiers, semantic web, linked open data (LOD) [9], and cross-origin resource sharing (CORS) are examples of possible ways to commonly map objects within confederated systems. The sensitivity of each object also needs to be commonly established between parties, though, so trust between domains can be fully incorporated, including authorization control.

Separation of duties

The ability to control and divide system functions so single users cannot perform certain system activities (those not specific to their professional duties) is particularly important in health care. That’s because system functions can offer functionalities that represent conflicts of interest if conducted by the same user. These functions/tasks should therefore be specifically mapped within the system to allow conflict identification. The first task is to locate or create checkpoints along the system flow and processes to help enumerate user responsibilities and accountabilities. Users able to insert health planning and request treatment procedures to be executed should not be those able to authorize them or forward provider reimbursement in case of insurance or government payers-based healthcare systems. That’s because requesting and authorizing functions denote clear conflict of interest. Function-based privilege management can be asserted upon legislation, professional regulation, or other task-oriented specifications to achieve separation of purpose due to legal, ethical, or other conflict. Manual identification of conflict of functions, while composing roles for later assignment, is an administrator task and prone to error. This is a very sensitive process and requires additional care leveraging separation of duties (SoD) in EHR systems.

RBAC was created with SoD in mind. Static separation of duty (SSoD) and dynamic separation of duty (DSoD) components can be used natively to separate functions that can be performed by single users. The use of static and dynamic components is referred to as RBAC restrict mode. Static validations are performed by system security administrative tasks while creating new roles. Dynamic validations may be needed during system use to identify conflicted roles on user’s sessions in case of multiple role assignment. The second case needs particular attention on EHR systems, a common scenario in the case of users with multiple roles assigned being prompted to choose which role is to be used in the current session. The problem arises when the EHR system fails to map the history of user action in such a SoD-protected function [10] so in the next session an error is not alerted if that user selects a different role that alone shows no conflict. Dynamic SoD is commonly determined to be not compliant on security audits when such behavior is discovered.

Access delegation

Access delegation (user grants) is also related to accountability and professional regulation issues and can make use of dynamic access control capabilities. In this case, slightly different from previously described problems, user discretion is used to forward grants temporarily to another user with the intention of allowing treatment to continue in case of his absence. An EHRs feature for that purpose usually allows part or all user grants to be “delegated” to the chosen user.
For instance, an IT user responsible for backup operations on the system could allow another user to perform these actions. In this case, necessary training is required. Notice, though, that for some type of users (healthcare professionals, for instance) this operation must be accompanied by role vetting, considering the professional title or other identification, because the accountability in this case is legally bound to the healthcare procedures that the professional is authorized to perform. A possible solution to this specific access control threat could be adding a table or ontology/taxonomy that describes healthcare specialties (i.e., American Board of Health specialties [11]) and related professional tasks/duties in a way that could be later translated to an existing system function list for additional access control decisions. Using this suggested flow, a grant delegation will be processed only if role and professional duties match: a physician could never delegate his granting to an IT user for instance. In figure 2, USER2 can delegate grants to USER3 but not to USER1 due to professional duties restrictions incorporated into the authorization access decision.

Conclusions

Role-based access control (RBAC) is the most prevalent access control method mediating healthcare professionals on EHR systems. Emergency access, access-delegation, cross-border scenarios, PHI privacy control, least privilege, and separation of duties are examples of security challenges to access control in the healthcare industry. Some can be addressed using native security components of RBAC, while others require adaptations. Variations of the RBAC original components and the use of hybrid models or mixed RBAC extensions are possible solutions found in research literature to cope with health informatics specific scenarios when it comes to authorization access issues.

Update our survey

Please consider updating our Brazilian survey with an international perspective of the current use and future expectation for access control implementation on electronic health record systems. Our English-translated survey can be found here. When prompted, please provide the following #ID: 435348-2 that characterizes respondent profile as an ISSA Journal reader.

References


About the Author

Marcelo Carvalho, CISSP, CISA, CRISC, has 17 years of information security experience at telecom and digital certificate companies and is currently an IS auditor for information assurance security and a IT/IS professor at various universities. He may be contacted at marcelo.carvalho@ieee.org.