Health Information Compliance Alert

Security: Get Staff Rolling With Role-Based Access Control

Stop unauthorized PHI disclosures before they start with 'RBAC.'

If you don't limit the amount of confidential data your staff can access, how can you ensure that unauthorized disclosures of medical information don't occur?

Implement a Role-Based Access Control (RBAC) model to determine who has access to your organization's medical data files.

Access control is the, "collection of mechanisms that specifies what users can do, which resources they can access and what operations they can perform on a system,"says **Uday O. Ali Pabrai,** CEO of **HIPAAAcademy** and **www.ecfirst.com.** RBAC is just one example of an access control technique; it follows HIPAA's, "minimum necessary" provision and bases disclosures of confidential data on job function.

Your role: That means your organization must decide who requires access to confidential data (protected healthinformation, for example) to do their job, and exactly what type of information they require.

Specifically, this means you must identify:Those persons or classes of persons, as appropriate, in your workforce who need access to confidential information to carry out their duties; and for each such person or class of persons, the category or categories of confidential information to which access is required and any conditions appropriate to such access, says Pabrai.

Authentication Vs. Access Control

Authentication refers to the identity of the user; it's the ability to prove or validate the identity of a user or a transaction. Access control refers to what the user can do and what the user can access. "The objective of access control is to implement technical policies and procedures for electronic information systems that maintain business information to allow access only to those persons or software programs that have been granted access rights," says Pabrai.

With RBAC, rather than attempting to map an organization's security policy to a relatively low-level set of technical controls (typically, access control lists), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role, explains Pabrai. That means a user is associated with a role, and roles are associated with permissions. "A user has permission only if the user has an authorized role which is associated with that permission," he notes.

How Does It Work?

Each staff member is assigned one or more privileges that are permitted to those in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning members of the workforce to the proper roles.

Getting Started With RBAC

1. The first step in implementing RBAC is to define all roles within your organization. "Keep in mind that some roles may be permanent, such as, "department head," while others may be temporary roles such as, "consulting security specialist," notes Pabrai. Once roles are identified, you should review them on a regular basis.

2. Each role is a class of users that have similar access rights. Each individual is assigned a role or roles and receives certain rights and privileges associated with that role.

3. After the role inventory is complete, perform a complete inventory of all of your active applications. There may be various types of data and this would need to be classified based on factors such as type and sensitivity. Examples of data types may be administrative, test results and others, while examples of sensitivity may include records related to HIV or mental health, which may have stricter access requirements than other PHI.

The Bottom Line: 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 having similar access rights, RBAC can provide significant security management efficiencies within your organization, says Pabrai.