Health Information Compliance Alert

SECURITY: HERE'S HOW TO GIVE 'ACCESS CREEP' THE OLE HEAVE-HO

Expert guidance to help you streamline your access procedures

Do you have a method to evaluate and update your staffers' access privileges after a promotion?

If you can't answer that question, your organization is probably suffering from "access creep" - and you aren't alone.

Access creep is a common problem that happens "as a person moves from one job to another and picks up the access privileges for their new position without losing the privileges from their old position," explains **Steve Wiggin**, a security analyst in Omaha, NE.

This piling on of access could continue as people moves through your organization - allowing them to view a plethora of information and possibly putting you in the security rule hot seat. But you can clamp down on access creep with a few changes to your access control policies and procedures, experts say.

Here are a few methods to ensure your employees never retain more access than they need to do their jobs:

1: ASSIGN GROUP ROLES, NOT INDIVIDUAL RIGHTS

Role-based access control (RBAC) is a good foundation for controlling your staffers' access privileges, says **Greg Young**, information security officer for Mammoth Hospital in Mammoth Lake, CA. RBAC allows you to create standard, generic profiles that you can then customize as needed.

"The theory behind RBAC is that people change more than job responsibilities do, so you assign people to a certain role and that role has a defined set of access permissions," Wiggin says. For example, the profile for Nurse will have different access privileges than the profile of Billing Clerk, regardless of the person filling the roles.

When a person's status within your organization changes - say they move from Nurse to Administrator or from Billing Clerk to Billing Department Supervisor - you can adjust their level of access by taking away the old role and assigning the new one.

Important: In order for RBAC to work, you must hammer out exactly what roles exist in your organization. "We have three basic roles that we layer as needed: enterprise-wide, job/team-specific and cross-functional," Wiggin shares.

Enterprise-wide access is given to every full-time employee and includes privileges like e-mail, while job-specific access is assigned to teams and is based on what they need. Cross-functional access is reserved for employees who are in transition from one role to another or who need access across teams, such as a LAN administrator or an executive.

2: MAKE DEPARTMENTS ACCOUNTABLE

If an employee is moving from department to department, you can place responsibility for updating the staff member's access privileges on the individual units, says **Leslie Gibb,** information security administrator of MCG Health in Augusta, GA.

For example, if a staffer is moving from the medical records department to the billing office, the records department supervisor would have to revoke the staffer's access before the billing office can assign the employee any access.

"It becomes a matter of accountability," Gibb says. "The first department does not want to continue to assume responsibility for someone who no longer works for them," and it ensures that the second department's access configuration is correct.

3: PLACE PRIORITY ON ACCESS MAINTENANCE

Strong access maintenance procedures can catch access creep before it has a chance to run rampant, Wiggin notes. "The problem is people are busy and maintenance is the last thing that gets done," he explains.

Best practice: Ask your department managers to evaluate their teams' access privileges every six months or when a person transfers to another unit, Wiggin recommends. Then you should assess each user's access privileges at least annually.

THE BOTTOM LINE

No matter how you attempt to stop access creep in your office, you must establish strong lines of communication between clinical, administrative and technology departments, Young stresses. For example, your human resources department should quickly notify your IT team if a person's status changes so that you can make changes to their access rights.

Failure to address and eliminate access creep in your organization could lead to a staff member having inappropriate access to your patients' PHI - and that could land you with a violation.