Codify
BY AAPC

Health Information Compliance Alert

Case Study: Level Your Role-Based Access Playing Field In 3 Easy Steps

Professional advice helps you avoid access landmines.

There is no perfect way to grant role-based access, but the easier your approach is to implement, the better. Here's how one privacy pro tackled the access beast in her organization.

The problem: "We have three different facilities with different staff sizes," says **Susie Honeycutt**, privacy officer and transcription supervisor with Kingsport, TN's Cardiovascular Associates.

And while the job titles at each site were the same, the job descriptions varied according to how staff members at each facility split the workload. For example, front line staffers in Kingsport have the same access level as those in Bristol, but because Bristol employees double up on duties, they also have full clinical access.

The solution: Honeycutt took the following three steps to create a flexible role-based access policy that works for each facility.

Step 1: Set up incremental access levels. Starting with Level A, Honeycutt ranked access from full to none. For example, Level A grants full access and modification privileges to all PHI, but Level C allows full access and no modification privileges.

Step 2: Ask department supervisors to assign access levels. Rather than grapple with each job's access needs, Honeycutt delegated this responsibility to the department heads. The supervisors grant access to the job description -- not individual employees, she stresses. For example, Insurance Clerk 1 has full access and Insurance Clerk 2 has Level B access regardless of the person filling those roles.

Step 3: Make room for exceptions. Honeycutt created a temporary access policy to deal with emergency situations when personnel must step into others' job roles (see "Avoid Detours On The Road To Role-Based Access" later in this issue). The policy also applies to the times when staff members hold multiple titles, she notes.

The bottom line: No matter what method you use to grant role-based access, remember to review your users' access needs periodically, Honeycutt says. Take care of any instances of inappropriate access before they jeopardize your compliance, she urges.