Health Information Compliance Alert

Compliance Strategy HAVE YOU TAKEN 'ROLE' CALL YET?

With the privacy rule finalized and the security regs on their way, covered entities are scrambling to get their ducks in a row. But did you know that setting up role-based access controls could help you kill two of these birds with one stone?

Under 45 CFR §142.304 of the proposed security standards, the U.S. Department of Heath and Human Services suggests role-based access controls (RBAC) as a model for regulating electronic information access within an organization.

With RBAC, "each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role," reports HHS.

According to attorney Robyn Meinhardt of Foley & Lardner in Denver, CO, entities which establish role-based access controls could find that the task "dovetails nicely with the minimum necessary requirements" of the HIPAA privacy rule.

The privacy regs' minimum necessary standards require covered entities to identify "those persons or classes or persons, as appropriate, in its workforce who need access to protected health information to carry out their duties," as well as "the category or categories of protected health information to which access is needed and any conditions appropriate to such access," as stated in 45 CFR §164.514.

The list of job classes or PHI categories that must be drafted under the minimum necessary requirements can provide a good starting point for determining what roles exist within your organization, suggests Meinhardt. "For each job category, the entity has to decide what protected health information that person needs in order to do their job," she says. This, in turn, should provide an understanding of the different roles within your facility that require PHI access. At that point, it then becomes a matter of defining these roles and categories in your organization's policies, Meinhardt directs.

What Have You Got Already?

Determining which employees perform what roles for your facility isn't as daunting as it sounds, says Margret Amatayakul, president of Margret A. Consulting in Schaumburg, IL.

Most entities should begin to define job categories and access controls by looking at what classification systems they currently have in place, offers Amatayakul.

More often than not, entities with a Human Resources department or system will find that position codes already exist within their organization.

"So you may have an HR system that identifies several different categories of nurses, or several different categories of other workers," which depending on facility size and type might constitute "between 15 and 25 job codes or position codes," she explains.

Amatayakul says entities can then examine these codes from the standpoint of RBAC and ask, "Ok, do we need to go beyond that or not?"

Don't Mess With Treatment

Once you've established the job duties for a given role, "you need to take reasonable steps to limit access for people who fulfill that role to only the information they need" to perform that job, according to attorney Michael Roach with Michael Best & Friedrich in Chicago.

CPT® 2023 American Medical Association. All rights reserved.

When defining roles and limiting PHI access, however, entities should be certain that their policies do not obstruct or inhibit a patient's treatment in any way. HHS is "very concerned that these privacy rules not stand in the way of providing treatment for patients," remarks Meinhardt.

Both Roach and Meinhardt agree that to ensure proper patient treatment with RBAC, entities should aim to limit a physician's access to PHI with training and policy, and not with log-ins and passwords. "It certainly seems to be acceptable under the proposed security rules to limit access based on policy, rather than technology," suggests Meinhardt.

To this end, HIPAA training and compliance policies must clearly instruct physicians to access only the health records of patients for which they are caring, reminds Mienhardt. Or doctors who remain confused over the issue of PHI access can benefit from Roach's maxim: "Use it when you need it. Otherwise don't."

CPT® 2023 American Medical Association. All rights reserved.