Health Information Compliance Alert

COMPLIANCE: 4 STRATEGIES TO HELP YOU GRANT ROLE-BASED ACCESS

You can stamp your patients' PHI 'for authorized eyes only' - here's how

Role-based access is the best way to keep PHI out of unauthorized staffers' reach, but it can be challenging to implement. Use these methods to assign role-based access in your organization without breaking your back-or your compliance plan.

1. MAP HOW YOUR PHI FLOWS

One way to figure out who needs to see your patients' health information is to pinpoint how it moves through your facility, notes **Stephen Priest**, a health care consultant with Professor Steve & Associates in Bedford, NH.

You need to know "who must view PHI, who is responsible for updating it" and each stop it makes along the way, he says.

Tip: Use the TPO test to sort out any access confusion. Ask yourself: What level of access will serve a treatment, payment or health care operations purpose?

No TPO purpose means limited access, Priest stresses. For example, a staffer who must view medical records won't necessarily need the ability to change the information contained in them.

2. ATTACH ACCESS TO JOB DESCRIPTIONS

You don't have to purchase complicated computer systems to dole out access, says **Susie Honeycutt**, privacy officer for Cardiovascular Associates in Kingsport, TN. Instead, take a look at your job descriptions and ask yourself "how much access do your employees have and how much do they need?" she suggests.

Get started: Use your risk assessment to determine whether each employee's current level of access is appropiate, Priest advises. Then build access rights into employees' job descriptions, he adds.

But don't expect each employee's role to fit perfectly into your existing job descriptions to better match what our staff members were actually doing," she explains. Bonus: This process will help you get a handle on - and better represent - your workflow, Priest says.

3. TRACK BACK TO ACCESS

Your audit logs provide a real-time picture of what information your staffers access in the course of a day or week, Priest affirms. You can track accessed PHI back to your users to root out what information they can be cut off from, he says.

Check out these examples:

Scenario A: Your audit logs show that a billing staffer accessed a patient's lab reports. You and the billing department supervisor determine that the staff member needed to view the report to determine which codes should be applied. Therefore, you decide the billing staff should have access to clinical information in the future.

Scenario B: Your logs show that a laboratorian accessed several patients' billing information, including birth dates and Social Security numbers. With the lab director's input, you decide the staffer had no treatment-, payment- or health care

operations-based need to view that info. His access is denied.

This strategy is not without flaws, points out **Matt Simon**, manager of security for Emory Healthcare in Atlanta. You have to spend large chunks of time researching whether instances of non-standard access are either inappropriate or exceptions to the written job function, he cautions.

4. BASE ACCESS ON OBJECTIVE STANDARDS

"We use human resources' information and job titles rather than job descriptions," Simon says. That's because job descriptions tend to be very subjective. "Someone has to decide what each person does and what they need access to," he explains.

With an objective approach, you tie the job description to the job title and department, which creates a holistic picture of the actual work performed.

"There are so many job functions in a hospital that sometimes we overestimate what people can do," he says. By eliminating some of that subjectivity, you can accurately grant the level of access your personnel will use - not what you think they might use.

THE BOTTOM LINE

As with all job roles, exceptions will happen whether someone's hired to do a specific job that changes over time or one employee is filling in for another, Priest assures. Your policy must be able to accept and adapt to those changes.

Update your access levels whenever job descriptions or department functions change, Priest reminds. Tip: Review your job descriptions and access levels during your annual training and any time a staff member leaves her position, he suggests.