

Role Based Access

What is “role based access”?

It means that the organization allows levels of access to protected health information (PHI) based on individual roles or job duties.

Does this apply to staff and faculty?

Yes, and also to students, residents, fellows, and volunteers—anyone who accesses protected health information to do his/her job.

Why do we need to designate levels of access?

Everyone should not have the same level of access to PHI. Some people will have greater access based on their job duties than others.

Does HIPAA require that we establish a role based access?

Yes, the Privacy Rules state, under the Minimum Necessary Requirements standard (164.514 (d) (2)),

(i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified (above—(A)) to protected health information consistent with (above—(B)).

In addition, the HIPAA Security Regulations also address limiting access through Workforce Security (164.308 (a) (3)) and Information Access Management (164.308 (a) (4)) standards.

How does a department or clinic comply with these standards?

First, you need to determine what PHI you have in your department and/or clinic and then evaluate each individual in your department and/or clinic and determine the level of access each needs to do his/her job. This means not looking at the access they may currently have but determining what access they need.

There is very little electronic PHI in my department, making access very open to the paper information. How can I limit access to paper information?

Some access controls are as simple as providing rules for the department/clinic and educating staff, faculty, etc., on access limitations. Certainly it is easier to limit access to electronic PHI for programs where passwords can be given to only those with the right to access, and it is easier to monitor inappropriate access to electronic systems with auditing capabilities. However, by setting rules in your department and/or clinic you establish a basis for expectations and accountability.

Why doesn't Human Resources just decide who can have access to various categories of PHI by job title?

Job titles and actual duties vary significantly from department to department. An Administrative Assistant II in one area may deal directly with patients and patient information, whereas an AAI in another area may rarely be exposed to PHI as part of normal job duties. Operations also vary in that some departments have very few staff, and although their titles may vary, they may function in similar capacities.

Okay, this is something that I need to do. Where do I start?

Attached are forms that may help you with this process. Listed along the left side are samples of types of PHI that you may have in your area, as well as various access limitations. Along the top are samples of job titles. Department and/or clinic leadership should work together both to identify the types of PHI within the department or clinic and to determine appropriate access based on individual department and/or clinic needs and operations.

What about other confidential information in my area, such as personnel or student information?

You may want to go ahead and add these categories to the form, although not specifically required at this time.

What do I do with the forms when we complete them?

You need to designate someone in the department/clinic to maintain them if ever needed for audits or reviews or to assist in the event that you have an access incident in your area. The forms do not need to be updated unless access limitations change or a new employee is added.

Do I have to use these forms?

No. If you have another method of designating access (narrative, a different form, etc.), you may use it, if it clearly outlines allowed access for each job title in your area.

Do you have some guidance on what appropriate access should be?

Again, this should be specific based on the operations of each department or clinic, but attached is an example. Generally, few individuals should have open access to all patient or billing records, whether paper or electronic. You should be able to explain access decisions that you make for your area.