Appropriate System Access Control Guidelines

SUBJECT: Appropriate System Access Control Guidelines

FROM: IU School of Medicine, Security Office

25 February 2005

This letter will provide guidance on establishing appropriate system access control for users and administrators of computer systems. This guidance is based on university and school policies and also the requirements of the Health Information Portability and Accountability Act (HIPAA).

Guidance provided by Indiana University IT policy IT-12, Security of University IT Resources states that organizational units (campuses, departments, offices, affiliated agencies, etc.) operating technology resources are responsible for ensuring that those systems are managed securely. Among other things, securely managing technology resources is described by the university policy as limiting access to needed services to authorized persons only and that day-to-day work should normally be accomplished as a non-privileged user. The School of Medicine follows university policy and guidelines related to the issue of access control of users.

The HIPAA security rule also provides guidance related to access control of users of technology resources where ePHI may be present. The following sections of the rule apply directly to access control:

Access Control §164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

Access Authorization §164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

Access Establishment and Modification §164.308(a)(4)(ii)(C): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Based on the above guidance, the IU School of Medicine Security Office recommends special attention should be provided to access controls of any technology resources managed by a department, specifically any resources where ePHI may be present. Appropriate access control would include limiting administrative account access of resources based on job function and tightly controlling access of outside parties, vendors, and other non-affiliated members of the department. For example, personnel responsible for computer server maintenance and operation would normally not require administrative-level access to the department's workstations.
Likewise, personnel whose primary job function is desktop maintenance would not require administrative-level access to the department's servers. Under normal circumstances, the user's job function will dictate the type and level of access required. In some cases where personnel need administrative-level access to both servers and workstations, the department should carefully evaluate the request and document the deviation. This deviation should be granted only in rare circumstances though.

Any further questions can be directed to this office by calling 317-278-8751 or email erschmid@iu.edu