**AS—04 Information Access Management**

***Purpose***

To manage the authorization of access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. 164.308(a)(4)(i)

**Guidance**

Restricting access to only those persons and entities with a need for access is a basic tenet of security. By implementing this standard, the risk of inappropriate disclosure, alteration, or destruction of ePHI is minimized. Covered entities must determine those persons and/or entities that need access to ePHI within their environment.

**Isolating Healthcare Clearinghouse Functions**

Implementation: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. 164.308(a)(4)(ii)(A)

**Access Authorization**

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

* There must be a formal system for authorizing user access to ePHI, such as an account request form requiring management approval.
* Access is to be granted in accordance with a role-based approach.
* Maintain documentation of all authorized users of ePHI and their access levels.
* Employees must receive security awareness and HIPAA training prior to obtaining access to ePHI.
* HIPAA systems must have the capacity to set access controls.

**Access Establishment and Modification**

Implementation: To develop 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. 164.308(a)(4)(ii)(C)

* Develop and implement procedures to establish, document, review and modify a user’s access to ePHI. Access shall use the principle of “least privileges”.
* Procedures must ensure regular review of those with access to ePHI, including the appropriateness of access levels.
* Procedures must require prompt initiation of account modifications/termination.