The Termination of an Employee

TERMINATION PROCEDURES (A) - § 164.308(a) (3) (ii) (C)

Where the Termination Procedures implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

> "Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section."

The purpose of this procedure is to comply with the HIPAA Security Rule's requirements pertaining to the integrity, confidentiality, and availability of electronic protected health information (ePHI).

This policy covers all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all ePHI, which is available currently, or which may be created, used in the future. This policy should apply to all employees and non-employees who collect, maintain, use or transmit ePHI in connection with all activities of your practice.

Termination procedures must be implemented to remove access privileges when an employee, contractor, or other individual previously entitled to access information no longer has these privileges. Whether the employee leaves the organization voluntarily or involuntarily, procedures to terminate access must be in place.

The same process that is implemented for termination should also be used to change access levels if an employee's job description changes to require more or less access to ePHI. The procedures should also address the complexity of the organization and the sophistication of associated information systems.

For the termination procedures implementation specification, covered entities and business associates should address implementing procedures for terminating access to electronic PHI when the employment of a workforce member ends or their role changes.

Why, you ask. Termination procedures are relevant for any covered entity or business associate with employees, because of the risks associated with the potential for unauthorized acts by former employees, such as acts of retribution or use of proprietary information for personal gain. The purpose of termination procedure documentation is to ensure that termination procedures include security-unique actions to be followed, for example, revoking passwords and retrieving keys when a termination or reassignment with different access privileges (for example from clinical to non-clinical, etc.) occurs.

MRC needs to know when an employee has been terminated or a change of access is needed. We want to help your Practice to be HIPAA Compliant.