§ 164.310 Physical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) Implementation specifications:

(i) Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

§ 164.312 Technical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access