TMA Privacy Office Information Paper

Facility Access Controls

HIPAA Security◆ November 2003

Standard Requirement

Covered entities must implement facility access controls as a part of their physical safeguards. The HIPAA Security Rule defines that as “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.”

This standard requires limiting physical access both to all buildings or business suites and to areas dedicated to the storage and use of computer equipment and media. Physical access controls should permit entry to individuals with appropriate authorization and deny entry to individuals lacking appropriate authorization. These physical controls reinforce both the administrative and technical policies and procedures on information access management required elsewhere in the rule. The administrative, physical, and technical controls collectively protect the confidentiality, integrity and availability of protected health information by permitting only authorized individuals to create, review or modify only information for which they have a “need-to-know”.

Implementation Specifications

Four implementation specifications are included in this standard, all of them addressable:

- contingency operations,
- facility security plan,
- access control and validation records, and
- maintenance records.

Because these implementation specifications are addressable, compliance depends on the outcome of a covered entity’s information security risk assessment.

The first implementation specification, contingency operations, embraces the establishment — and if necessary implementation — of “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.” (Both plans are required implementation specifications under the contingency plan standard.) Some overlap exists between contingency operations under “Facility Access Controls” and contingency planning under “Administrative Procedures”. This rule focuses attention on the functioning of the facility and its access control mechanisms (both administrative and technical) during and after an emergency or disaster. A covered entity should include evaluating threats to the correct functioning of physical access controls during an emergency and during efforts to recover from disasters as part of its information security risk assessment. A covered entity must document its plans for assuring appropriate physical access during emergencies and disaster recovery efforts in its risk management plan.

The second implementation specification, facility security plan, includes policies and procedures “to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.” A covered entity must evaluate the need for, and adequacy of controls on physical access to facilities and equipment handling protected health information as part of its information security risk assessment. As part of its risk management plan, a covered entity should document its approach to controlling physical access to facilities and equipment handling protected health information. A good facility security plan will include policies, procedures and practices that always and only provide authorized, necessary access to health information assets during routine and emergency operations.

The third implementation specification, access control and validation procedures, relates to policies and procedures that “validate a person’s [physical] access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.” This is the physical equivalent of the “need to know” information access limits described by the minimum necessary rule. As part of its information security risk assessment, a covered entity must evaluate the need for procedures that provide individuals’ physical access only to the “minimum necessary” data they “need-to-know” in order to discharge their job responsibilities. As part of their information security risk assessment, covered entities should evaluate the need for policies and procedures for the following access controls;

1. Validating identity and access authorizations of people requesting access to a building, suite, controlled rooms and/or computer equipment prior to allowing access;
2. Controlling the flow of visitors through its facilities including patients, vendors, visitors and guests;
3. Permitting only authorized personnel to enter a site where software programs are tested and revised.

Their risk management plan must justify their decision and explain any physical access controls adopted on the basis of that principle. This rule complements the access control requirement found in the category, “Administrative Procedures”. Under the “Administrative Procedures” category, covered entities must implement controls that establish different levels of access to information depending on work needs. From the perspective of the user, controlling physical access to areas within the facility with “need-to-know” procedures supports and strengthens the protective function of differentiating levels of general access to information stored and processed within the facility.

Taken together, the second and third implementation specifications could include such measures as sign-in and/or escort for visitors to the areas of the facility that contain information systems hardware or software. But this would depend on the covered entity's particular circumstances. While some sort of physical access control is obviously necessary for every facility, the particulars will vary considerably.

The last implementation specification, maintenance records, covers 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). As part of their information security risk assessment, covered entities should evaluate the need for keeping a record of the repairs and modifications to the physical components of a facility housing electronic protected health information (EPHI). The risk management plan should document the results and justify all actions taken in response to the risk assessment. Such procedures ensure accountability and aid in maintaining the facility security plan and other safeguards.

As with all the other specifications, policies and procedures are required to be "formal, documented" ones. If a covered entity does not control the building they occupy or shares space with other organizations, it nonetheless remains responsible for considering facility security. DHHS has noted that a covered entity retains a responsibility for considering building security even when it shares space within a facility used by other organizations. (Final Rule, p.8353) If facility security is in part based on the efforts of third parties (e.g., the building's own security force), that must be documented. And, of course, such reliance must be "reasonable and appropriate" to the circumstances. The covered entity can incorporate security measures into contracts with the party responsible for the building and document them in their own facility security plan.

See also:
45 CFR 164.310(a)(1)

Federal and DoD regulations that support this standard
DoDR 5200.8
DoD 8510.1-M
DoDI 8500.2