



Security Incident Procedures

HIPAA Security ♦ November 2003

Standard Requirement

As part of their [administrative safeguards](#), covered entities must implement policies and procedures to address security incidents. This standard requires a covered entity to develop a plan for handling security incidents and breaches. The [Security Rule](#) defines a security incident as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.” ([164.304](#)) Some examples of security incidents include policy violations by users, denial of service attacks, intrusions, and unauthorized disclosures.

Implementation Specification

This standard has one [implementation specification](#), which is required. “Response and reporting” includes three steps:

- Identification and response to suspected or known security incidents;
- Mitigation, to the extent practicable, of harmful effects of security incidents that are known or suspected; and
- Documentation of the incidents and their outcomes.

Each covered entity must document how it will identify, respond to and document an incident. These response procedures should be developed for all levels of incidents. Incidents may have many critical short and long-term effects on an organization. An organization’s initial response to an incident may have a big impact either helping or hindering short and long-term impacts. It is very important for the covered entity to document any incidents, how they responded to the incident, and the impact on its operations. This is to ensure that all security violations are reported and handled quickly. The specific documentation processes and appropriate responses “will be dependent upon an entity’s environment and the information involved.” (Final Rule, p.[8350](#)) External reporting is not addressed by the standard because it is governed by other business or legal considerations, such as any requirements of state law. As part of a compliance review, DHHS might ask to see security incident documentation.

See also:

[45 CFR 164.308\(a\)\(6\)](#)

Federal and DoD regulations that support this standard

[OMB A-130 App. III](#)

[DoDI 5215.2](#)

[DoD 8510.1-M](#)

[DoDI 8500.2](#)