
45 C.F.R. § 164.308

Administrative safeguards.

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

(1)

(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) *Risk management (Required).* Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) *Sanction policy (Required).* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(D) *Information system activity review (Required).* Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3)

(i) *Standard: Workforce security.* Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase Login](#)