

**(15)(i) Objective.** Protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities.

**(ii) Measure.** Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary.

Sec. 164.308 Administrative safeguards.

(a) A covered entity must, in accordance with Sec. 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.

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

(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.

