



Audit Controls

HIPAA Security ♦ November 2003

Standard requirement

Covered entities must implement audit controls as a part of their [technical safeguards](#). The [Security Rule](#) defines this requirement as implementation of “hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use [electronic protected health information \(EPHI\)](#)”

Covered entities must select and implement a technical service to document system activity. This provision lays the groundwork for the audit requirement found in [administrative safeguards](#). While [§ 164.308\(a\)\(2\)\(v\)](#) under “Administrative Safeguards” requires covered entities to review the records produced by the audit mechanism, this standard requires covered entities to install and use an audit mechanism. This standard does not state what should be audited. Organizational policies, risk assessments, good industrial practice and other regulations such as the privacy standard determine a covered entity’s choice and pattern of auditing events. “Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses.” ([Final Rule, p.8355](#)) While there is flexibility in determining what should be audited, all standards must be met and audit mechanisms must be implemented. There are no associated implementation specifications with this standard.

See also:

[45 CFR 164.312\(b\)](#)

Federal and DoD regulations that support this standard

[DoD 8510.1-M](#)

[Controlled Access Protection Profile](#)

[DoDI 8500.2](#)