



Policies and Procedures

HIPAA Security ♦ November 2003

Standard requirement

This standard requires covered entities to implement “reasonable and appropriate” policies and procedures to comply with HIPAA data security standards and implementation specifications. Covered entities must take into account the specific conditions of their individual situation as discussed in the General rules and, thus, ground their approach to HIPAA compliance in risk management. In deciding which security measures to use, a covered entity must take into account the following factors:

1. The size, complexity, and capabilities of the covered entity.
2. The technical capabilities of record systems used to maintain electronic protected health information.
3. The costs of security measures.
4. The probability and criticality of potential risks to electronic protected health information.

A covered entity may not use compliance with this standard as an excuse for violations of the other HIPAA security standards. A covered entity may change its policies and procedures as long as the changes also do not violate the requirements of the other HIPAA security regulations and are documented. There are no associated implementation specifications with this standard.

See also:

[45 CFR 164.316\(a\)](#)