



## Managing Information Privacy & Security in Healthcare

### HIPAA Final Standards for Data Security

By Jeff Collmann, PhD and Ted Cooper, MD

The HHS published the Final HIPAA Security Standards in the Federal Register on February 20, 2003. These standards cover 49 pages in the Federal Register; however the standards and implementation specifications themselves require only seven pages. The other pages explain the HHS response to comments on the Notice of Proposed Rulemaking and provide a matrix of the security standards and implementation specifications.

The Final HIPAA Security Standards apply to the same covered entities as the Final HIPAA Privacy Standards: health plans, healthcare clearinghouses, healthcare providers who transmits any health information in electronic form in connection with a HIPAA standard transaction. However, the Security Standards apply only to electronic protected health information. They do not apply to oral or paper protected health information.

Covered entities must:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Standards.
4. Ensure compliance by its workforce.

The approach to compliance is meant to be flexible.

1. Covered entities may use any security measures that enable the covered entity to reasonably and appropriately implement the standards and implementation specifications.
2. In deciding which security measures to use, a covered entity must take into account the following factors:
  - a. The size, complexity, and capabilities of the covered entity.
  - b. The covered entity's technical infrastructure, hardware, and software security capabilities.
  - c. The costs of security measures.
  - d. The probability and criticality of potential risks to electronic protected health information.
1. The implementation specifications are either required or addressable.

2. When a standard includes required implementation specifications, a covered entity must implement the implementation specifications.
3. When a standard adopted has addressable implementation specifications, a covered entity must:
  - a. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and
  - b. As applicable to the entity:
    - (1) Implement the implementation specification if reasonable and appropriate; or
    - (2) If implementing the implementation specification is not reasonable and appropriate
      - (a) Document why it would not be reasonable and appropriate to implement the implementation specification; and
      - (b) Implement an equivalent alternative measure if reasonable and appropriate.

Security measures implemented to comply with standards and implementation specifications adopted must be reviewed and modified as needed to continue provision of reasonable and appropriate protection electronic protected health information.

The standards and implementation specifications are arranged in three sections:

1. Administrative safeguards,
2. Physical safeguards, and
3. Technical safeguards.