



HIPAA Security Standards, the Final Rule

The final security standards for HIPAA were published on February 20, 2003. Under this rule, health insurers, certain health-care providers, and health-care clearinghouses who qualify as covered entities must establish procedures and mechanisms to ensure the confidentiality, integrity and availability of electronic protected health information (ePHI). The rule requires covered entities to implement **administrative, physical, and technical safeguards** to protect electronic protected health information that they create, receive, store, or transmit.

Most covered entities had two full years – until April 21, 2005 -- to comply with the standards required by HIPAA.

Key Features of the Final Rule

The security standards are:

- **Scalable** - All covered entities must implement these standards. In determining how to apply the standards, covered entities should take into account their size, complexity, capabilities, costs of complying with the standards, and the potential risks to their electronic protected health information.
- **Technology neutral** -The standards do not specify any particular technology. They outline what must be done, not how to do it.
- **Designed to protect electronic data whether it is in storage, being actively accessed and updated, or transmitted to another location:**
 - **Administrative safeguards** - management of the selection and execution of security measures.
 - **Physical safeguards** - protections for electronic systems, related buildings and equipment from environmental hazards and unauthorized intrusion.
 - **Technical safeguards** - automated processes to protect data and control access to it.

Security Rules Dovetail with Privacy Requirements

The security standards work in concert with the final privacy standards adopted by HHS, which took effect for most covered entities on April 14, 2003. The two sets of standards use many of the same terms and definitions in order to make it easier for covered entities to comply.