

Frequently Asked Questions About Security and Electronic Signature Standards

1. What is the purpose of the new Security and Electronic Signature standards?

The new standards have been developed to protect the confidentiality, integrity, and availability of individual health information.

2. Why were new Security and Electronic Signature standards needed?

No existing standard provides uniform, comprehensive protection of individual health information. HIPAA mandates new security standards to protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. HIPAA also mandates that a new electronic signature standard be used where an electronic signature is employed in the transmission of a HIPAA standard transaction.

3. What problems do these standards address? solve?

The new Security Standard will provide a standard level of protection in an environment where health information pertaining to an individual is housed electronically and/or is transmitted over telecommunications systems/networks. The Electronic Signature Standard will provide a reliable method of assuring message integrity, user authentication, and non-repudiation.

4. How will the standard protect individual health information?

The standard mandates safeguards for physical storage and maintenance, transmission, and access to individual health information.

5. How will the new standard be implemented?

Implementation will depend upon numerous factors, e.g., the configuration of the entity implementing it, the technology it employs, and the risks to and vulnerabilities of the information it must protect.

6. Who must comply with the Security Standards?

Any health care provider, health care clearinghouse, or health plan who electronically maintains or transmits health information pertaining to an individual.

7. Who must comply with the Electronic Signature standard?

Any health care provider, health care clearinghouse, or health plan that employs an electronic signature in the transmission of one of the transactions adopted under HIPAA.

8. Do security requirements apply only to the transactions adopted under HIPAA?

No. The security standard applies to individual health information that is maintained or transmitted. This is a much broader reach than the specific transactions defined in the law. The electronic signature standard applies only to the transactions adopted under HIPAA.

9. Is the use of an electronic signature mandatory?

No. None of the transactions adopted under HIPAA requires an electronic signature at this time.

10. Do the Security Standards apply to hardcopy, e.g., paper documents, as well as to electronic information?

No. The standards apply to individual health information in electronic form only.

11. Why doesn't the Security Standard select specific technologies to be used?

To select a specific technology to satisfy the security requirements found in HIPAA would tend to bind the health care community to systems and/or software that may soon be superseded by rapidly developing technologies and improvements. The Security Standard was developed with the intent of remaining "technologically neutral" to facilitate adoption of the latest and most promising developments in this dynamic field and to meet the needs of health care entities of different size and complexity. The security standard is a compendium of security requirements that must be satisfied. The particular solution will vary from business to business but each will meet the basic requirements.

12. How could a small provider implement the security standard?

The proposed security standard does not require extraordinary measures to implement. It involves taking actions that a prudent person would agree were necessary to assure the security of the information to be protected. The standard does not dictate specific technologies. The requirements of the standard may be implemented in a number of ways, depending upon the security needs and technologies in place at each business and upon agreements among businesses that work together.

The Notice of Proposed Rule Making (NPRM) includes an example to illustrate the manner in which a small provider might implement the standard. We expect that those required to implement the standard would first assess their security risks and vulnerabilities and the mechanisms currently in place to mitigate those risks and vulnerabilities. Following this assessment, they would determine what additional measures, if any, need to be taken to meet the security requirements.

Source: <http://aspe.hhs.gov/admsimp/fqsec.htm>
U.S. Department of Health and Human Services
Administrative Simplification: Privacy and Security