

Answer ID 1854
Topic HIPAA Administrative Simplification
Category HIPAA Admin. Simplification
Date Created 03/24/2003 08:09 AM
Date Updated 08/12/2004 02:52 PM

Is mandatory encryption in the HIPAA Security Rule?

Question

Is mandatory encryption in the HIPAA Security Rule?

Answer

No. The final HIPAA Security Rule made the use of encryption an addressable implementation specification. See 45 CFR §§ 164.312(a)(2)(iv) and 164.312(e)(2)(ii). Covered entities use open networks such as the Internet and e-mail systems differently, and no single interoperable encryption solution for communicating over open networks exists. Setting a single encryption standard could have placed an unfair financial and technical burden on some covered entities.

The encryption implementation specification is addressable, and must therefore be implemented if, after an assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its environment. If the entity decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate, or if the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure.