

## **HIPAA Security FAQs**

### *1-Is mandatory encryption in the HIPAA Security Rule?*

No. The final 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.

### *2-What is encryption?*

Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

### *3-Does the HIPAA Security Rule allow for sending electronic protected health information (PHI) in an email or over the Internet? If so, what protections must be applied?*

The Security Rule does not expressly prohibit the use of email for sending electronic PHI. However, the standards for access control, (45 CFR § 164.312(a)) integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against the unauthorized access to electronic PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect electronic PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for electronic PHI to be sent over an electronic open network as long as it is adequately protected.

*4-Do the HIPAA Security Rule requirements for access control, such as automatic logoff, apply to employees who telecommute or have home-based offices if the employee accesses electronic protected health information (PHI)?*

Yes. Covered entities that allow employees to telecommute or work out of home-based offices and have access to electronic PHI, must implement appropriate safeguards to protect the organization's data. The automatic logoff 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 logoff 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.

The information access management and access control standards, however, require the covered entity to implement policies and procedures for authorizing access to electronic PHI and technical policies and procedures to allow access only to those persons or software programs that have been appropriately granted access rights.

*5-What is the difference between Risk Analysis and Risk Management in the HIPAA Security Rule?*

Risk analysis is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic PHI held by a covered entity, and the likelihood of occurrence.

The risk analysis may include inventorying of all systems and applications that are used to access and house data, and classifying them by level of risk. A thorough and accurate risk analysis would consider all relevant losses that would be expected if the security measures were not in place, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage.

Risk management is the actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising its electronic PHI and to meet the general security standards.

*6-What is a system vulnerability?*

A system vulnerability is a flaw or weakness in a system, due to its design, installation, lack of policies and procedures, or some other cause. Any of these weaknesses, whether intentional or accidental, could potentially result in a breach or inappropriate use or disclosure of electronic PHI. Some vulnerabilities may be caused by ineffective policies regarding user or log on IDs and passwords, holes or weaknesses in some of the software tools, or flaws in the operating system, application or inadequate access controls.

*7-How will we know if our organization and our systems are compliant with the HIPAA Security Rule's requirements?*

The purpose of the final rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic PHI that is collected, maintained, used or transmitted by a covered entity. Compliance is different for each organization and no single strategy will serve all covered entities.

Covered entities should look to § 164.306 of the Security Rule for guidance to support decisions on how to comply with the standards and implementation specifications contained in §§ 164.308, 164.310, 164.312, 164.314, and 164.316. In general, this includes performing a risk analysis; implementing reasonable and appropriate security measures; and documenting and maintaining policies, procedures and other required documentation.

Compliance is not a one-time goal, it must be maintained. Compliance with the evaluation standard at § 164.308(a)(8) will allow covered entities to maintain compliance. By performing a periodic technical and nontechnical evaluation a covered entity will be able to address initial standards implementation and future environmental or operational changes affecting the security of electronic PHI.

*8-Are we required to “certify” our organization’s compliance with the security standards?*

No, there is no standard or implementation specification that requires a covered entity to “certify” compliance. The evaluation standard § 164.308(a)(8) requires covered entities to perform a periodic technical and nontechnical evaluation that establishes the extent to which a entity’s security policies and procedures meet the security requirements.

The evaluation can be performed internally by the covered entity. There are also external organizations that provide evaluations or “certification” services. A covered entity may make the business decision to have an external organization perform these types of services. It is important to note that HHS does not endorse or otherwise recognize private organizations’ “certifications,” and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a “certification” by an external organization does not preclude HHS from subsequently finding a security violation.

*9-Does the Security Rule apply to written and oral communications?*

No. The Security Rule is specific to electronic PHI. It should be noted however that electronic PHI also includes telephone voice response and faxback systems because they are used as input and output devices for computers. Electronic PHI does not include paper-to-paper faxes or video teleconferencing or messages left on voice mail, because the information being exchanged did not exist in electronic form before the transmission. In contrast, HIPAA Privacy Rule address all mediums of PHI, including written and oral. Information on the Privacy Rule can be found online at: <http://www.hhs.gov/ocr/hipaa/>.

*10-What does the HIPAA Security Rule mean by physical safeguards?*

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The standards under physical safeguards include facility access controls, workstation use, workstation security, and device and media controls. The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems whether such systems are housed on the covered entity's premises or at another location.

*11-Does the HIPAA Security Rule mandate minimum operating system requirements for the personal computer systems used by a covered entity?*

No. The Security Rule was written to allow flexibility for covered entities to select the technology that best fits their organizational needs. The Security Rule does not specify minimum requirements for personal computer operating systems, but it does mandate requirements for information systems with electronic PHI. Therefore, as part of the information system, the security capabilities of the operating system may be used to comply with technical safeguards standards and implementation specifications such as audit controls, unique user identification, integrity, person or entity authentication, or transmission security.

*12-Does the HIPAA Security Rule require the use of an electronic or digital signature?*

No, the Security Rule does not require the use of electronic or digital signatures. However, electronic or digital signatures could be used as a security measure if the covered entity determines their use is reasonable and appropriate.

Additionally, the final rule to adopt a HIPAA standard for electronic signatures has not yet been published. Consequently, the implementation of an electronic signature standard currently is not required.

*13-Are covered entities required to use the National Institute of Standards and Technology (NIST) guidance documents referred to in the preamble to the final HIPAA Security Rule?*

No. Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.