Explanation of Sample HIPAA Privacy Policy Number 8: Minimum Necessary and Reasonable Safeguards

Covered entities, including physician practices, are required by the Privacy Rule to use reasonable safeguards to limit uses and disclosures beyond that which is the minimum amount necessary to accomplish the intended purpose. This explanation and sample HIPAA Privacy Policy 8 discuss the obligations of practices to comply with the minimum necessary standard and to apply reasonable safeguards to limit uses and disclosures to that which is minimally necessary for a permitted purpose under the HIPAA Privacy Rule.

Minimum Necessary

The Privacy Rule requires that protected health information only be used or disclosed when it is necessary for treatment, payment, or health care operations. The "minimum necessary standard" requires covered entities to look at uses and disclosures of protected health information and limit the amount of information used or disclosed to the minimal amount that is necessary to achieve the purpose of the use or disclosure. Practices are required to identify those individuals within the practice who require access to protected health information and determine categories or types of protected health information that is needed and the conditions upon which the information should be accessed.

The minimum necessary standard does not apply to treatment related communications to or from a health care provider. The standard also does not apply when the individual patient is asking for copies of or access to his or her own information. Where a disclosure is required by the HIPAA rules or by law, the minimum necessary standard is likewise inapplicable.

Routine uses or disclosures of information (such as disclosures to a health plan for payment) should be subject to standard operating protocols. Non-routine uses or disclosures must be evaluated on a case by case basis to determine the appropriate amount of information that should be disclosed.

Reasonable Safeguards

In order to prevent inadvertent disclosures beyond those which meet the minimum necessary standard as set forth above, the Privacy Rule requires covered entities, including physician practices, to apply "reasonable safeguards" when using or disclosing protected health information to reduce the risk of "incidental disclosures" (e.g., overheard conversations, etc.). In recognizing that all incidental uses and disclosures cannot be eliminated in a health care setting, the HIPAA Privacy Rule provides that, if reasonable safeguards have been applied, then certain incidental disclosures will not be considered a violation. The applicable standard that is applied in determining whether a safeguard is "reasonable" is whether a prudent health care professional would deem the safeguard to be "reasonable."

Although all identifiable patient information is considered "protected health information" for purposes of HIPAA, more sensitive information is generally considered to require greater safeguards in order to be considered "reasonable." For example, a voicemail message with an appointment reminder for a dentist office may be considered reasonable while a voicemail appointment reminder for an HIV clinic may not be. This should be taken into account when reviewing the sample policy and adapting it for use in a physician practice.

The reasonableness of safeguards is also dependent on the size and resources of the practice. While the costs associated with a particular safeguard may be considered reasonable for a hospital, the same safeguards may not be considered reasonable for a small physician practice.

The requirement to reasonably safeguard protected health information applies to oral, written and electronic information. However, electronic protected health information must also be protected pursuant to the specific administrative, physical and technical specifications of the HIPAA Security Rule.