

RE: **THE HIPAA SECURITY RULE**

Dear Healthcare Provider:

On February 20, 2003, the Department of Health and Human Services issued the final version of the HIPAA Security Rule. The Security Rule is the third component of HIPAA. The Security Rule is intended to work in concert with the Privacy Rule by expanding the obligations of covered entities. Covered entities that maintain electronic protected health information (“EPHI”) must take additional precautions to maintain the integrity, confidentiality and availability of EPHI.

Who is a Covered Entity under the Security Rule?

Because the Privacy and Security Rules are intended work together, the definition of a covered entity is the same under both rules. Therefore, all health plans, health care clearinghouses and health care providers who transmit any health information in electronic form are covered entities under the Security Rule. A covered entity under the Privacy Rule is a covered entity under the Security Rule.

If I am a Covered Entity, what am I required to do to comply with the Security Rule?

The Security Rule requires covered entities to take the “reasonable safeguards” required under the Privacy Rule a step further to protect EPHI. EPHI includes all protected health information that is created, received, maintained or transmitted in electronic form. Electronic form includes information created electronically (e.g. patient information your workforce inputs into a computer system), received electronically (e.g. electronic communications from patients, other healthcare providers or health plans) maintained electronically (e.g. patient medical records or other individually identifiable patient information contained in a computer system) and information that is transmitted in electronic form (e.g. transmitted patient claim information electronically to your billing company). The Security Rule does not apply to information in paper or oral format.

Under the Security Rule, covered entities are required to implement administrative, physical and technical safeguards to protect EPHI. Similar to the Privacy Rule, the Security Rule is flexible and is based upon a sliding scale of compliance. Therefore, the safeguards your practice implements will be appropriate for the size and the needs of your practice based upon how your particular practice creates, receives, maintains and transmits EPHI. Also, the Security Rule is technology neutral, and does not mandate either the adoption of electronic creation, receipt, maintenance and transmission of protected health information or the use of a particular brand or type of technology.

Generally, the Security Rule requires covered entities to protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, protect against any reasonably anticipated uses or disclosures of EPHI which are not permitted by the Privacy Rule and ensure that your workforce is trained and capable of achieving compliance with the Security Rule. Like the Privacy Rule, the Security Rule requires covered entities to adopt written policies and procedures for your practice in order to comply with the Security Rule.

The Security Rule sets forth implementation specifications that fall into the general categories of administrative, physical and technical safeguards. In keeping with the Security Rule's flexibility approach, certain implementation specifications are "required" and certain implementation specifications are "addressable." The required implementation specifications are actions your practice *must* do in order to comply with the Security Rule; if you do not implement the required specifications, you cannot be in compliance with the Security Rule. The addressable implementation specifications are ones that your practice must, after a risk analysis, consider implementing if appropriate and necessary. If after an evaluation, you determine that it is not appropriate to implement an addressable implementation specification, your entity must document this decision and reasoning in addition to any alternative safeguards your practice adopted instead.

Finally, the Security Rule permits a covered entity to contract with a third party in order to create, receive, maintain or transmit EPHI. In keeping with the terminology of the Privacy Rule, these third parties are also known as "business associates" under the Security Rule. Similar to the Privacy Rule, if your practice uses a business associate to create, receive, maintain or transmit EPHI, you must receive satisfactory assurances that your business associate will maintain the integrity, confidentiality and availability of your patients' EPHI. These satisfactory assurances will be given in the form of a business associate agreement you are required to enter into with any third party who creates, receives, maintains or transmits EPHI on your behalf

What is the compliance deadline?

The deadline for compliance with the Security Rule is April 21, 2005. While this date seems far away, for a couple of reasons, it is important to adopt an early understanding of the Security Rule. First, since the Privacy Rule and Security Rule work hand-in-hand, you may want to consider implementing the requirements of the Security Rule in the near future to supplement and enhance your existing Privacy Rule policies and procedures. Second, if your entity is considering upgrading its technology, it should consider the requirements of the Security Rule at this time rather than trying to retrofit the new technology to achieve compliance with the Security Rule.