HIPAA PRIVACY AND SECURITY RULES

As part of overall changes associated with the Affordable Care Act and the Health Information Technology for Economic and Clinical Health ("HITECH") Act there have been some changes to various rules associated with privacy and security. These changes may require covered entities to amend their Business Associate Agreements or other aspects of their operation. Along with these changes, there is an increase in the focus on ensuring compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") rules.

Therefore, this Provider Alert is to serve as a reminder to all providers of the importance of ensuring compliance with the Privacy and Security Rules. As an example, in a recent case a managed care company agreed to pay HHS a substantial sum to settle potential HIPAA violations that were caused by security weaknesses during a process to modify an online application. From the HHS site:

OCR's investigation indicated that WellPoint did not implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule. The investigation indicated WellPoint did not:

- adequately implement policies and procedures for authorizing access to the on-line application database
- perform an appropriate technical evaluation in response to a software upgrade to its information systems
- have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database.

As a result, beginning on Oct. 23, 2009, until Mar. 7, 2010, the investigation indicated that WellPoint impermissibly disclosed the ePHI of 612,402 individuals by allowing access to the ePHI of such individuals maintained in the application database. This data included names, dates of birth, addresses, Social Security numbers, telephone numbers and health information.

Whether systems upgrades are conducted by covered entities or their business associates, HHS expects organizations to have in place reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of electronic protected health information – especially information that is accessible over the Internet.

Therefore, HIPAA covered entities (which includes healthcare providers) who may be developing web-based applications or portals used to provide access to Members’ health data using the internet must ensure that appropriate administrative and technical safeguards, as required under the HIPAA Security Rule, are implemented to protect ePHI before using such Web-based applications or portals.