



April 2007

### HIPAA UPDATES — PRIVACY COMPLIANCE, SECURITY AUDITS AND NPI DEADLINE / CMS CONTINGENCY PERIOD

**HIPAA Privacy Compliance.** Five years after the enactment of the HIPAA Privacy Rule, complaints to the U.S. Department of Health and Human Services Office of Civil Rights (OCR) continue to be filed against all types of Covered Entities, with the total approximately 24,000 through 2006. The good news is that OCR still appears to be in an educational/voluntary compliance mode. OCR has not levied any civil penalties against Covered Entities for non-compliance, although it has referred more than 360 complaints to the Department of Justice for possible criminal prosecution, with 39 accepted. In view of the ongoing filing of complaints, Covered Entities are best served by continuing to monitor their HIPAA Privacy policies and procedures, revising them as needed and documenting their efforts. [See page 2 on guidelines for Handling HIPAA Privacy Complaints]

**Security Rule Compliance Audits.** Covered Entities subject to the HIPAA Security Rule must be diligent in their compliance efforts, since government audits have started. As it stated in its 2007 Work Plan, the Department of Health and Human Services' Office of Inspector General (OIG) believes that while the increasing use of electronic medical records in the health industry will promote economy and efficiency in the delivery of health services and enhancement of patient safety, the downside is an ever increasing concern over the privacy and security of patient health information. Consequently, the OIG has started to audit hospitals for Security Rule compliance, with its first such audit involving a Georgia hospital. The OIG has not disclosed its basis for selecting which Covered Entities to subject to a compliance audit, although it does not appear that these initial audits are in response to any patient complaint of non-compliance by the facility.

**NPI Deadline/CMS Contingency Period.** May 23, 2007

is the final deadline for HIPAA health care providers to obtain a National Provider Identifier (NPI). By then, such providers must include the NPI on all of their health care claims electronically submitted to payers or else face rejection of the claims.

However, CMS recently announced that it will not enforce the NPI deadline for up to one year if a non-compliant provider can demonstrate its good faith efforts to come into compliance. The provider may also be required to submit a corrective action plan. On a case by case basis, CMS will determine if there is reasonable cause for the provider's noncompliance and the extent to which a cure period is appropriate. Obtaining an NPI prior to the NPI deadline will be a key component to demonstrating good faith efforts, even if the provider lacks the ability to use the NPI. CMS has stated it will use a flexible voluntary compliance approach, with enforcement actions being complaint-driven. Guidance on compliance after the NPI implementation deadline is available on CMS's website at [www.cms.hhs.gov](http://www.cms.hhs.gov).

CMS's issuance of an NPI contingency plan for Medicare is expected any day. Other payers are expected to issue their own contingency plans, none of which will be allowed to have an extension period greater than one year from the NPI deadline. Consequently, non-compliant providers may have to deal with multiple NPI contingency plans.

It is still not too late for providers to apply for an NPI. It can be done online at [www.nppes.cms.hhs.gov](http://www.nppes.cms.hhs.gov) or a paper application is available by calling CMS at 1-800-465-3203. There is no cost for obtaining an NPI. Once obtained, the provider should begin to share it with its payers, including Medicare, and document its efforts in the event they cannot meet the NPI deadline. As CMS says, "Get It, Share It, Use It".