

May 2006

*Mokena: 19065 Hickory Creek Drive, Suite 220, Mokena, IL 60448 (708) 479-3230
Bloomington: 1003 Martin Luther King Drive, Bloomington, IL 61701 (309) 827-6026*

HIPAA UPDATE
May 2006

**Federal Regulations and Other
Related Documents**

**DOJ Issues Opinion on HIPAA Criminal
Enforcement**

In June 2005, the Department of Justice (“DOJ”) issued an opinion at the request of the Department of Health and Human Services’ general counsel and the senior counsel to the deputy attorney general in the Justice Department. The opinion involved clarification of the scope of section 1320d-6, which deals with criminal enforcement of violations of patient privacy. The opinion restricts prosecutions of such violations to: covered entities; certain directors, officers and employees of such covered entities who may be criminally liable directly in accordance with general principles of corporate criminal liability; and third parties who cause, aid or abet, counsel, command, induce, procure, or conspire with, a covered entity to act (through employee conduct imputed to the entity in certain circumstances) in violation of HIPAA. The opinion states that, if the covered entity is not an individual, the liability of the entity and individuals’ within the entity will be determined by general principles of corporate criminal liability. According to corporate criminal liability general principles, certain directors, officers, and employees of covered entities may be directly liable. Those who cannot be held directly

liable may nonetheless be held liable pursuant to principles of aiding and abetting liability and of conspiracy liability. Based on corporate liability doctrines, prosecution will occur if the employee of an entity acted with some intent for the entity’s benefit. The DOJ opinion declined to discuss in greater detail the general corporate and aiding and abetting principles, noting the law varies in different jurisdictions and will be applied on a case by case basis.

**CMS Posts NPI Information for Medicare
Organization Provider Subparts**

The Centers for Medicare and Medicaid Services (“CMS”), in January 2006, adopted a final rule (the “National Provider Identifier (“NPI”) Final Rule”), which adopted the NPI as the standard unique health identifier for health care providers for use in HIPAA standard transactions. On or prior to May 23, 2007, all covered entities (except small health plans) must obtain and use NPIs to identify themselves as “health care providers” in the HIPAA standard transactions that they conduct with Medicare and other covered entities. Such organizations also need to determine if they have “subparts” that need NPIs. A subpart needs to have its own NPI.

The goal of adopting subparts is to help promote smoother and more efficient Medicare claims processing during the implementation of the NPI in the Medicare program. Further, the determination of subparts is necessary to ensure entities within a covered organization health care provider that need to be uniquely identified in HIPAA standard

transactions obtain NPI's for that purpose. The following statements apply to all entities that could be considered subparts:

1. A subpart is not itself a separate legal entity, but is a part of a covered organization health care provider that is a legal entity. (All covered entities under HIPAA are legal entities.)
2. A subpart furnishes health care as defined at 45 CFR 160.103.

In addition, the following may relate to an entity that a Medicare covered organization health care provider could consider as subparts:

1. A subpart may or may not be located at the same locations as the covered organization health care provider of which it is a part.
2. A subpart may or may not have a Taxonomy (Medicare specialty) that is the same as the covered organization health care provider of which it is a part.
3. Federal statutes or regulations pertaining to requirements for the unique identification of enrolled Medicare providers may relate to entities that could be considered subparts according to the discussion in the NPI Final Rule.

As an example, an enrolled provider (a hospital) owns 10 home health agencies, all operating under the TIN of the hospital. Because the hospital and each of the 10 home health agencies is separately surveyed and enters into its own provider agreement with Medicare, a total of 11 unique NPI's should be obtained.

Medicare is transitioning from the provider identifiers it currently uses to NPI's. Therefore, it is imperative that organization health care providers obtain NPI's to replace the identifiers currently being used in order to continue to conduct transactions with Medicare.

CMS FAQ Answers

Two new HIPAA questions were added to the FAQ's section of the CMS website on February 14, 2006.

The first question asks "In the absence of a final rule, may trading partners agree to use electronic transactions and attachments to support both business-to-business processes until the HIPAA standards for electronic health care claims attachments are adopted?" CMS answers that, in the absence of HIPAA standards for electronic health care claims, trading partners may use appropriate industry standard to conduct a transaction, in accordance with a trading partner agreement.

The second questions asks "What types of business structures are considered organization health care providers and thus eligible for organization NPI's? What types are not?" CMS states that it has applied the following guideline to determine if an entity is eligible for a NPI: Any organization that is recognized by the State as separate and distinct from the individual is eligible for an organization NPI. Therefore, sole proprietorships (where one person owns all the assets of a business) cannot get an organization NPI. The law in each state will govern how different business types are recognized by the state.

Health Plan Member Notification

CMS reminded health plans that, if a health plan is a covered entity under HIPAA (most are), notification must be sent to health plan members in some manner by **April 14, 2006** of the availability of the health plan's Notice of Privacy Practices.

Final HIPAA Enforcement Rule Published

The final rule, effective March 16, 2006, establishes procedural and substantive requirements relating to the imposition of civil money penalties on covered entities that violate a HIPAA provision or rule (*see* 71 Federal Register

32). It also amends the existing rules relating to the investigation of noncompliance to make them apply to all of the HIPAA Administrative Simplification rules, rather than exclusively to the privacy standards. In addition, it clarifies and elaborates upon the investigation process, bases for liability, determination of the penalty amount, grounds for waiver, conduct of any hearings and the appeal process.

Proposed Rule for Standards for Electronic Health Care Claims Attachments

On September 23, 2005, the Department of Health and Human Services (“DHHS”) published this proposed rule adopting standards for electronic health care claims attachments (*see* 70 Federal Register 184). The proposed standards discuss ways to electronically request and supply particular types of additional health care information in the form of an electronic attachment to support submitted health care claims data. The rule proposes using a combination of the X12N and HL7 standards, since X12N standards are used for exchanging administrative information and HL7 standards are used for exchanging clinical information, including a messaging standard to carry clinical information in a response transaction, and specifications for the content or “questions” that may be asked in different attachment types. It also proposes the adoption of the Logical Observation Identifiers Names and Codes (“LOINC”). LOINC is a new HIPAA code set that has codes for both laboratory results and clinical reports and includes codes for the attachment “questions” or requests proposed in this rule.

Related Illinois Legislation

Electronic Medical Records Taskforce

On July 29, 2005 Illinois created the Electronic Medical Records Taskforce and authorized the Taskforce to create a plan for the development and utilization of electronic health records in the state in order to improve the quality of patient care, increase the efficiency of healthcare practice, improve safety, and reduce healthcare errors (*see* Public Act 94-0646).