HIPAA INFORMATION SERIES

9. Final Steps For Compliance

This paper is the ninth in a series of informational papers developed by the Centers for Medicare & Medicaid Services (CMS) to communicate to the health care community key concepts and requirements contained in HIPAA -- the Health Insurance Portability and Accountability Act of 1996. This paper highlights the final steps for complying with the electronic transactions and code sets requirements.

Moving towards compliance

In the first eight papers, CMS outlines the steps providers must undergo to implement HIPAA’s electronic transactions and code sets standards. At this stage of HIPAA implementation:

☑ You have determined if you are a covered provider.

☑ You should be compliant with HIPAA’s privacy requirements.

☑ Your practice and your information systems are tested (or are in the process of being tested) and will be ready to conduct HIPAA compliant transactions effective October 16, 2003.

☑ You have identified your staff training needs and are implementing any necessary changes in operational policies and procedures.

☑ You are preparing to research other HIPAA provisions that may affect your practice.

Review the Transactions & Code Sets Modification Rule

This final rule published February 20, 2003 makes some important changes to the HIPAA electronic transactions and code sets standards that were published in August 2000. After the first regulation was published, many of the larger health care entities began the process of implementing the standards. It became clear that certain standards did not work for everyone and industry experts and HHS proposed changes be made to the regulation. This regulation is the result of that collaborative effort.
The primary change involves covered entities that bill drugs and biologics. In the original law the National Drug Code (NDC) was the adopted standard for doctors and hospitals, as well as for the retail pharmacy sector. Industry groups and Government experts concluded that, at this time, the National Drug Codes would be too expensive for hospitals and doctors to implement and would not enhance their business processes. This regulation repeals the National Drug Code standard for those entities. The National Drug Codes will remain the standard for the retail pharmacy drug claim, and there will be no standard code set adopted for non-retail pharmacy drug claims. Based on this appeal, we would expect hospitals and doctors to continue to code and bill drugs and biologics using their current practices.

**What are the addenda?**

Changes to the initial electronic standards were adopted in the February 20, 2003 Modification Rule. The modifications were approved by industry groups and facilitate implementation of the adopted standards. These changes are detailed in documents called “addenda.” The addenda supplement the original implementation guides, which provide the technical details for each standard. The original implementation guides for HIPAA’s electronic transactions and code sets are known as version 4010. The subsequent addenda are referred to as version 4010A. For more information on the implementation guides and addenda for the transactions providers use most frequently, see paper 4 in this series, “Overview of electronic transactions and code sets.”

**Stay tuned for the Medicare Electronic Billing Requirement final rule**

Effective October 16, 2003, HIPAA law requires that all claims submitted to Medicare be submitted electronically in the HIPAA standard format (with the exception of those from certain small providers and under other limited circumstances.)

The rule detailing the new Medicare electronic billing requirement is currently being finalized. You will receive more information on this provision in upcoming Medicare provider bulletins. You may also sign up for the HIPAA regulation ListServe that will notify you when any HIPAA rules are published: [http://www.cms.hhs.gov/hipaa/hipaa2/regulations/lsnotify.asp](http://www.cms.hhs.gov/hipaa/hipaa2/regulations/lsnotify.asp).
Unique identifiers requirements

HIPAA also requires the use of unique identifiers to clearly identify entities within the health care delivery system. The Provider Identifier Standard Final Rule and the Health Plan Identifier Proposed rule are in the process of being finalized. Once adopted, these identifiers will be used in HIPAA transactions.

Plan for the security requirements

The security standards work in concert with the final privacy standards adopted by HHS last year. The two sets of standards use many of the same terms and definitions in order to make it easier for covered entities to comply. The final security standards for HIPAA were published on February 20, 2003. Under this rule, health plans, payers, clearinghouses, and certain health care providers must establish procedures and mechanisms to protect the confidentiality, integrity and availability of electronic Protected Health Information (PHI.) Most covered entities will have two full years – until April 21, 2005 – to comply with the standards; small health plans will have an additional year to comply.

Review the final security standards

As the health care industry evolves and continuously relies upon the use of technology, the security standards will play an important role in protecting electronic data at rest and in transit. The standards were developed to promote the protection of electronic protected health information by:

- Providing for electronic data integrity and confidentiality,
- Allowing only authorized individuals access, and
- Ensuring its availability.

The security standards are scalable and technology neutral. This means that covered entities should take into account their size, complexity, capabilities and potential risks to their electronic Protected Health Information when complying with the standards. The standards do not specify any particular technology. In other words, they outline what must be done -- not how to do it. The security standards require covered entities to implement safeguards within three categories:

TIP: The final National Employer Identifier Rule compliance date is July 30, 2004. The National Employer ID will use the Internal Revenue Service’s Employer Identification Number (EIN) for this number.

TIP: For a copy of the Security Rule and the Transaction and Code Sets Modifications Rule visit the CMS web site:
http://www.cms.hhs.gov/hipaa/hipaa2
行政保障 - 管理安全措施的选取和执行。

物理保障 - 对电子系统和相关建筑及设备的环境防护和未经授权的入侵防护。

技术保障 - 自动化过程对数据的保护和访问控制。

重点在运营改善

为了从HIPAA中获得最大利益，应该将焦点放在运营改善和长期业务战略上。HIPAA的行政程序简化要求可以成为对以下运营改善的催化剂：

- 更快、更简便、更准确的资格信息
- 减少因资格问题导致的拒付
- 加快获取预授权和转诊流程
- 减少因授权或转诊问题导致的拒付
- 提高提交声明的效率，减少错误和重新提交
- 取消地方代码的使用
- 使用相同的代码集与所有健康计划
- 从健康计划获得电子结算单
- “Auto-post”支付到您的系统 – 快速准确
- 电子请求声明状态信息
- 减少您的索赔处理成本，释放有价值的工作人员，同时保护健康信息的安全性和隐私。

登录CMS HIPAA网站并注册我们的ListServe：
http://www.cms.hhs.gov/hipaa/hipaa2

将您的问题发送至askhipaa@cms.hhs.gov

拨打CMS HIPAA热线 1-866-282-0659

HIPAA Deadlines

April 14, 2003
Privacy Deadline
(April 14, 2004 for small health plans)

April 16, 2003
Testing
You should start testing your software no later than April 16, 2003.

October 16, 2003
Electronic Transactions & Code Sets Deadline

NOTE: Medicare will require that all Medicare claims be submitted electronically, with the exception of those from small providers and under certain limited circumstances.

July 30, 2004
National Employer Identifier
(August 1, 2005 for small health plans)

April 21, 2005
Security Deadline
(April 21, 2006 for small health plans)

NOTE: Medicare will require that all Medicare claims be submitted electronically, with the exception of those from small providers and under certain limited circumstances.

April 21, 2005
Security Deadline
(April 21, 2006 for small health plans)