HIPAA UPDATE

EVERYTHING BUT PRIVACY

by

Edward F. Shay, Esquire

I. Introduction.

For the past three years, the sages of HIPAA have intoned that HIPAA is different from Y2K because it never goes away. They were right; but, arguably for the wrong reason. In the fullness of time, Y2K happened. In contrast, it seems that HIPAA almost never happens (on time).

Below is a review of what remains undone under the Administrative Simplification provisions of HIPAA, excluding privacy. Although enacted in 1996, HIPAA remains a work in progress. Several proposed rules have not been finalized. Other anticipated proposed rules have not been published. Final rules have not been timely modified to make them amenable to implementation on an industry wide basis. All of the above goes on in a sub-culture of organizations and acronyms that are unique to HIPAA. For example, transactions and codes sets get reviewed and updated by designated standard maintenance organizations, or “DSMOs.” The work of the DSMOs and other HIPAA interests groups is the frequent focus of hearings and reports by the National Committee on Vital and Health Statistics (“NCVHS”).

Most recently, Congress has enacted legislation to allow time to address some of the problems caused by implementation delays in HIPAA. Known as the Administrative Simplification Compliance Act, this legislative extension is discussed in section VI.

A. Proposed Rules that that are not final.

1. Health care provider identifier at 63 F.R. 25320 (5/7/98).

2. Employer identifier at 63 F.R. 32785 (6/16/98).


B. Standards under development as Proposed Rules.

1. Standard identifiers for health plans.

2. Standards for electronic claims attachments.

---


All rights reserved.
eshay@postschell.com
3. Modifications to Transactions Standards.


II. Status of Proposed but not Final Rules.

A. The Unique Provider Identifier. 66 F.R. 61193 (12/03/01)

   1. First proposed as an eight position, alpha-numeric identifier. Anticipated to change to ten position, nine digit all numeric identifier with one check position. Capable of enumerating 200 million providers with separate unique identifiers.

   2. Absent this standard, health plans will continue to assign their own provider numbering systems and providers will be required to maintain all of these identifiers.

B. Final Security Standards. 66 F.R. 61194 (12/3/01)

   1. Intended to establish administrative, technical, and physical safeguards to protect individually identifiable health information.

   2. Absent final security standards private industry will rely upon its own standards and it is believed that levels of security would be quite uneven. Further, because many events viewed as a breach of confidentiality or violation of privacy standards arise out of a failure of security, compliance with final privacy rules will be impaired by a lack of security standards.

C. Final Standards for Employer Identifiers. 66 F.R. 61195 (12/3/01)

   1. CMS has looked at various employer identification numbers but has not finalized a choice. No standard setting organization has undertaken this task.

   2. CMS believes that significant savings can be generated from an EIN and that lack of such an identifier will limit the full savings potential of standardized transactions.

III. Status of standards not yet published as Proposed Rules.

A. Modifications to Final Transaction Standards to repeal adoption of the National Drug Codes. 66 F.R. 61184 (12/3/01)

   1. The National Drug Codes (“NDC”) have proved largely unworkable and CMS is expected to repeal them as a standard. NCVHS
estimates that the cost of implementing the NDC alone could exceed the total cost of compliance with all other standard transactions. (See, NCVHS letter to Secretary Thompson, 2/22/01, Exhibit “A”).

2. The proposed rule may also adopt certain standards from the National Council for Prescription Drug Programs for certain retail drug transactions.

B. Health Care Claims Attachment Standards. 66 F.R. 61183 (12/03/01)

1. The claims attachment enables parties to electronic claims transactions to request and receive additional information about a pending claim.

C. National Standards for Identifiers for Health Plans. 66 F.R. 61182 (12/03/01).

1. A national identifier for health plans is a statutory requirement (§1173(b)). This proposed rule would move the standard setting process toward that objective.

D. Revisions to Transactions and Code Sets to enable Compliance. 66 F.R. 61182 (12/03/01).

1. The final transaction and code set regulations (65 F.R. 50312, 8/17/2000) established a review process for existing standards. This process is implemented through (“DSMOs”). DSMOs review changes needed to enable covered entities to comply with the regulation.

2. The DSMO review process identified 37 changes that must be made to enable covered entities to efficiently use the designated transaction standards. NCVHS reviewed these changes and recommended them to CMS in June, 2001. Transcript, Department of Health and Human Services, NCVHS, Subcommittee on Standards and Security (May 31, 2001). http://ncvhs.hhs.gov/010531tr.htm

IV. No Standards, no HIPAA.

As the foregoing suggests, there are significant developments pending in the implementation of HIPAA’s standardized transactions and code sets. Many believe that at this writing, it is unlikely that CMS would be able to move quickly enough to adopt new and revised standards on a timeline that would meet the transaction and code set compliance date of October 16, 2002.

A. Timeframes for change. 42 USC 1320d-3, imposes constraints on how and when standards can be adopted and modified.
1. In the first year of adoption, standards may only be modified as needed for compliance.

2. Thereafter, the Secretary may not modify or adopt standards more often than annually.

3. When modifying and adopting standards, the Secretary must consult with NCVHS and a host of industry groups.

4. Most recently, enactment of P.L. 107-105 (see, V infra) suggests that testing of modified transactions must be able to begin not later than April 16, 2003 to provide a six month run up to the October 16, 2003 compliance date.

B. When the foregoing timeframes are combined with the normal internal and external review periods for any type of rulemaking, it seem clear that CMS simply cannot publish proposed rules, obtain comments, publish final rules and have them in place before October 16, 2002 with any reasonable time period for testing.

C. Testing is critical. As the healthcare industry moves to adopt the standardized transactions and code sets, covered entities must acquire new claims processing software or translator software to interface with their existing programs. This software must adhere to the sometimes massive Implementation Guides (700+pages) for various standards. Before change of this magnitude can be implemented, it must be tested in two separate processes.

1. Certification Testing. In certification testing, a covered entity tests its software against a testing service offered by a third party vendor. See for example, the testing services available at www.claredi.com.

2. Partner to Partner Testing. Once trading partners have established that their systems produce HIPAA compliant transactions, they may still need to test on a partner to partner basis to work through systems compatibility issues such as adequacy of capacity, system security, or transmission integrity.

D. Industry impact.

1. NCVHS wrote to the Secretary of HHS:
   a. On February 22, 2001 advising the NDC was wholly unworkable. (See, Exhibit “A”).
   b. On June 29, 2001 advising that the DSMO “fast track” process had identified crucial modification that should clear the final rulemaking process not later than January 31, 2002. (See, Exhibit “B”).
2. On January 16, 2002, the American Hospital Association expressing concern for “numerous and ongoing delay” and “the problems this creates in meeting a compliance deadline.”

“All on behalf of the American Hospital Association's (AHA) nearly 5,000 member hospitals, health systems, networks, and other providers of care, I am writing to raise two sets of issues regarding the implementation of the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The first is a concern over delays in issuing the remaining regulations for electronic transactions standards and the problems this creates in meeting a compliance deadline. Closely related to these concerns are other unresolved implementation issues that also need to be addressed to facilitate timely compliance. The second is an opportunity for the Department of Health and Human Services (HHS) to take certain steps to assist health care providers in realizing the full savings and efficiencies potential implicit in the enactment of HIPAA through rulemaking or guidance to facilitate the prompt and accurate payment of claims.” (R. Pollack to the Hon. Tommy Thompson, http://www.aha.org/ar/Advocacy/)

3. Other industry views on the cost and complexity of compliance.

- I am Rich Landen. I am with the Blue Cross Blue Shield Association. I was invited to be on this afternoon's panel as a spokesperson for some individual Blue Cross Blue Shield plan employees who, individually or on behalf of their plan or on behalf of another organization, had submitted change requests through the DSMO process…..The number of service lines (in 837-I) supported and the maximum field sizes are a major concern and were not changed. (Transcript, Department of Health and Human Services, National Committee on Vital and Health Statistics, Subcommittee on Standards and Security (May 31, 2001). http://ncvhs.hhs.gov/010531tr.htm).

- I am George Arges, chairman of the National Uniform Billing Committee…. Item 128, physician information at the service line level. The issue, a request to remove all industry usage requirements for the reporting of physician information at the service line was made for data elements in loops 2420-A, 2420-B, 2420-C and D. Currently, institutional providers do not report physician or other care giver information at the line level. The rationale for removal is due to the enormous cost associated with having to comply with a set of requirements not necessary for claims adjudication, even though the guide defines this as situational usage. Although some provider system software can capture this information at the time care is
rendered to the patient, only a small percentage of these providers currently subscribe to this additional system feature from the service vendor, less than six percent. (Transcript, Department of Health and Human Services, National Committee on Vital and Health Statistics, Subcommittee on Standards and Security (May 31, 2001). http://ncvhs.hhs.gov/010531tr.htm).

- The HIPAA final rule of August 17, 2000 dealt Medicaid agencies a monumental blow. For years we had been encouraged to develop new services while continually being required to report such services in ever changing ways. The answer had always been to develop a local code that would pay the service correctly, pull funding from the proper account, and appropriately log the service for reporting purposes. For many states, the list of local codes had grown proportionately to their creativity in providing services or their budgetary requirements. In some cases states had thousands of locally developed codes to process the majority of their business. Loss of these codes would significantly handicap Medicaid’s ability to provide and report healthcare services to those with significant medical need. (The National Medicaid EDI HIPAA Workgroup, http://snip.wedi.org/public/articles/cracking.pdf.

V. Concerns About Industry Readiness.

A. Several recent industry surveys by HIMSS, HFMA and WEDI suggest that compliance with the TCS rules is layered along lines that suggests that:

1. Large sophisticated plans and providers are progressing with TCS compliance.

2. Smaller providers and their vendors are lagging significantly.

3. Key sectors are lagging; including Medicaid programs, Medicaid HMOs, long term care and self-funded employee health benefit plans.

B. Some of the compliance challenge may be attributable to the degree of change that a Covered Entity must accomplish to move from existing billing formats and information systems to TCS compliant transactions.

1. The CMS 1500 and CMS 1450 differ significantly from the TCS mandated 837 P and 837 I.

2. CMS 1500 “Relationship to Insured” allows four appropriate responses.
3.  837 P allows 25 appropriate responses.

4.  Compliance change management requires:

   • Enhanced back end information capture

   • Integration of enhanced information into current billing information systems. In this case from admissions process to billing process.

   • Formatting of information in compliance 837 P format.

C.  Many suspect, but do not know precisely, that significant sectors continue to rely heavily on paper claims formats, especially in the self-funded/TPA claims environment.

   1.  In general terms, paper claims may utilize 100 data elements while the 837 P and 837 I can average 300 data elements and require the ability to manipulate over 900 filed of data that may be required under varying circumstances.


   A.  In December, 2001, Congress passed H.R. 3323 and the President signed the ASCA.

   B.  How the ASCA Works.

   1.  The ASCA conditionally extends the compliance date for the TCS rules (Subparts I through R of 45 C.F.R. 162) from October 16, 2002 to October 16, 2003 for Covered Entities (i.e., health plans, providers and healthcare clearinghouses).

   2.  Covered Entities that want a compliance extension must:

       • Submit to the Secretary before 10/16/02
       • A “plan” of how to come into compliance by 10/16/03.

   3.  The plan is a “summary” of:

       • An analysis of the extent of, and reasons for a Covered Entity’s noncompliance by 10/16/02.
       • A compliance budget
       • A schedule
       • A work plan
       • A strategy for compliance
• Any plans to use contractors and vendors
• Timeframes for testing

4. By 3/31/02, the Secretary will develop a form for filing for an extension.

• Covered Entities may use their own form
• Electronic submissions will be permitted

C. How Compliance Plan’s May Be Used and Not Used

1. To document extension requests

• Significant authentication issues
• Significant volume issues

2. To provide to NCVHS information for analyses of effective solutions.

3. The ASCA protects some proprietary and identifying information; but it does not supersede the Freedom of Information Act, 5 USCA 552.

D. How Compliance Will Be Enforced.

1. The Secretary may exclude a Covered Entity from participation in Medicare after 10/16/02, if:

• No “plan in accordance with” the ASCA was filed; and,
• The Covered Entity is not in compliance with the TCS rules

2. All other HIPAA sanctions are preserved (e.g., fines and felonies).

E. Special ASCA Rules.

1. There is no TCS extension for small plans.

2. There is no change in the compliance date for the privacy rules.

3. There is no technical gap in privacy compliance relating to providers not transacting compliant TCS transactions.

4. Clearinghouses are deemed to be clearinghouses notwithstanding the delay.

F. Mandated Electronic Claims for Medicare.
1. The ASCA amended section 1862 of Title XVIII to exclude from coverage or payment any claim that is not submitted to the Secretary in an electronic form designated by the Secretary.

2. Exceptions may be granted:
   - When not electronic method is available
   - For “small providers” with 25 or fewer FTEs
   - For physicians with 10 or fewer FTEs

G. The ASCA authorizes $44 million for HIPAA/Non-privacy assistance, education and enforcement.

H. DHHS has released FAQs on the ASCA, attached here as Exhibit “D.”

VII. Seeking an Extension under the ASCA.

A. The Filing Requirement.

1. Applicant identifying information.

2. Required content is a plan that is a summary of:
   - Analysis of extent of non-compliance and reasons for it.
   - Budget requirements
   - Schedule
   - Work plan
   - Implementation strategy
   - Use of vendors or contractors to achieve compliance
   - Timeframe for testing to begin not later than 4/16/03.

3. Certification or attestation of submission?

4. Applicants are not required to use the model filing form. Under some circumstances, a customized form may make a stronger case for the applicant.
   - For example, a skilled nursing facility with a high Medicaid population may be more dependent on code changes (NDC, J-codes) than other types of delivery organizations. Here, the
lack of code set revisions would limit the ability of vendors to move the facility toward timely compliance.

B. The Non-summarized Plan. There should be a real plan with a real budget and work plan and strategy. Many covered entities already have a plan that guides their compliance efforts. Consider an ASCA specific update to document and substantiate an extension request.

1. Because the filing is a summary, then the ASCA implies that actual schedules, work plans and related documents must exist to substantiate the filing. If a certification or attestation is requested, then the actual documentation becomes a necessity.

2. Vendor support will likely be critical to many covered entities seeking an ASCA extension. A projection of the of the backlog in rulemaking suggests that virtually all covered entities may require an extension. The boom/bust cycle of transaction compliance may create serious shortages of qualified and reliable vendor support.

C. Relationship to overall compliance position. The ASCA adds yet another basis under Medicare for exclusion for many non-compliant covered entities. As covered entities assess their approach to the ASCA, they should do so in light of their overall compliance obligations and exposures.

1. Consider HCOs with corporate integrity agreements.
   - Would failure to file be a material violation?
   - Cannot possibly comply due to CMS’s inaction?

2. Consider HCOs in process of investigation. Has Congress handed the OIG or Justice a new and easy point of leverage?

3. Consider HCOs with established compliance programs. How does the compliance officer view the HCOs ability or lack thereof to implement the plan to conduct standardized transactions?

4. “It is essential that the compliance officer or other management officials immediately investigate reports or reasonable indications of suspected noncompliance. If a material violation of applicable law or compliance program requirements has occurred, a provider must take decisive steps to correct the problem.” (OIG Compliance Guidance for Nursing Facilities, 65 F.R. 14305, 3/16/00.

5. What will your auditors think? For the past two years, HIPAA compliance has been a perennial in most audit reports and in risk factor
D. Relationship to the rest of the industry. Can you afford to diverge from your trading partners?

1. The Department of Public Welfare Office of Medical Assistance Program (OMAP) is presently considering alternatives and options for meeting HIPAA readiness. A revised HIPAA implementation schedule, Frequently Asked Questions (FAQs) and Pennsylvania Medical Assistance HIPAA Billing Guides will be posted to this website in the near future. http://www.dpw.state.pa.us/omap/hipaa/omaphipaa.asp (2/08/02).

VIII. Health Information Security

In healthcare, confidentiality is a core value of the industry. For many stakeholders in the healthcare industry, confidentiality is a value often understood best in context, but less well recognized in its component parts. At a minimum, confidentiality involves policy choices about the use and disclosure of information. These choices are usually the substance of privacy rules. How policy choices get implemented is more often a matter of information security.

Security may be the least understood aspect of safeguarding information used and exchanged in healthcare. Some of security may involve choices of technology. For example, security may require choices about methods of encryption when an healthcare enterprise opts to transmit or receive sensitive information via the Internet. At other times, security may involve internal threats from rogue employees or warding off external attacks from hackers or viruses from infected email.


While there appears to be no agreed upon definition of "security" for healthcare purposes, some working definitions of the term are helpful to focus the issues. For example, the National Research Council defines "Security" as "the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats." (National Research Council, 1991).

Security is also defined in the proposed security rules under HIPAA's Administrative Simplification authorities. "Security": Security encompasses all of the safeguards in an
information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data. Glossary, proposed Security Regulations, 63 F. R. 43275, 8/12/98.


A legal obligation to maintain a state of security in an healthcare enterprise may arise from contractual terms of agreements between parties or from regulatory requirements. In the current environment, much of one's legal obligation to achieve and maintain security may depend upon the type of enterprise involved, the type of information to be protected or the nature of the activity in which the enterprise is involved. The leading legal bases for healthcare security are the following:

1. Proposed regulations by the Health Care Financing Administration under the Administrative Simplification provisions of HIPAA.

2. HCFA's current Internet Security policy for transmission of Privacy Act and other HCFA sensitive information.

Set forth below is a review of each.


A. As a somewhat unheralded component of HIPAA, the Health Insurance Portability and Accountability Act of 1996,2 Congress included Administrative Simplification ("AS"). AS involves a range of requirements aimed largely at improved electronic submission of claims and related financial transactions. 42 U.S.C. 1320d. Under the mandate of AS, "health plans,"3 "healthcare clearinghouses"4 and "health care providers"5 must comply with the

---

2 Subtitle F, Part C, P. L. 104-191. An earlier version of Administrative Simplification has been incorporated into the all-inclusive Health Security Act at Title V, Subtitle B.
3 A "health plan" may be a group health plan (includes insured and self funded), a health insurance issuer (e.g., insurance company), a health maintenance organization, Medicare, Medicaid, a Medigap policy issuer, some long term care policies, a multi-employer welfare benefit program health care for the active military, veterans health care, CHAMPUS, Indian Health Services FEHBP, State child health plans, Medicare+Choices program, other plans paying for medical care. 45 C.F.R. 160.103, 65 F. R. 82799 (12/28/2000).
requirements of the law. By regulation, these three types of entities are now referred to as "covered entities." Other elements of AS include unique identifiers for health plans, providers, employers and individuals. Under section 264 of HIPAA, the Secretary was also authorized to issue regulations on privacy protections for certain health information. Finally, AS authorizes the Secretary to promulgate regulations to enhance the security and confidentiality of health information.

In section (a) of section 262 of HIPAA, Congress enacted a new section 1173 of the Social Security Act. Section 1173 requires the Secretary to set security standards. In promulgating security standards, the Secretary is required to take into account several factors, including:

- the technical capabilities of record systems to maintain health information.
- the costs of security measures.
- the need for training persons who have access to health information.
- the value of audit trails in computerized record systems.
- the needs and capabilities of small healthcare providers and rural health care providers.

The Secretary is also required to insure that if health care clearinghouses are part of larger enterprises that the healthcare clearinghouse isolates its health information from the rest of the enterprise. Finally, Section 1173 states that all health plans, providers and healthcare clearinghouses must "maintain reasonable and appropriate administrative, technical and physical safeguards" to:

- ensure information integrity and confidentiality.
- protect against security threats to information.
- protect against unauthorized use or disclosure of information
- ensure compliance by officers and employees of covered entities.

In implementing the statutory directives of AS, the Secretary has promulgated a series of proposed rules and, at this writing, one final rule. The proposed rules have dealt with:

1. a health care provider identifier at 63 F. R. 25320 (5/7/98).
2. a standard employer identifier at 63 F. R. 32785 (6/16/98).

---

4 A "clearinghouse" is an entity, including a covered entity, that either (1) processes or facilitates the processing of nonstandard information into standard data elements; or, (2) receives a standard transaction from another entity and formats it into a proprietary/nonstandard format for transmission to a receiving entity. 45 C.F.R. 160.103, 65 F. R. 82799 (12/28/2000).

5 a health care provider as defined in 1861(u) or 1861(s) of Medicare or any other persons furnishing, billing or getting paid for health care services. 45 C.F.R. 160.103, 65 F. R. 82799 (12/28/2000).

Final regulations on standard transactions and code sets were published on August 17, 2000 at 65 F.R. 50312, and final regulations on health information privacy were published on December 28, 2000 at 65 F.R. 82462.

On August 12, 1998, HCFA published a proposed security regulations as part of the regulatory framework of the Administrative Simplification provisions of HIPAA, P. L. 101-104. In general, the proposed security rules present one of the most complete sets of security standards applicable to health care E-commerce. 63 F. R. 43242, 8/12/98.

Each health plan, health care clearinghouse, or health care provider must meet the security requirements of the proposed security regulations in transmitting, processing or storing "protected health information" electronically.

Because HIPAA applies to the electronic transmission or storage of "individually identifiable health information," HIPAA applies when that information is used, stored or transmitted over the Internet or stored in databases. Electronic transmissions would include transactions using all media, even when the information is physically moved from one location to another using magnetic tape, disk, or compact disc (CD) media. Transmissions over the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks are all included. 8

The proposed security standard sets forth four categories of requirements, as follows:

1. administrative procedures.
2. physical safeguards.
3. technical security services.
4. technical security mechanisms.

Each of the four categories will be addressed below.

B. Security Standard Requirements for Administrative Procedures.

1. Certification. A technical evaluation of an accreditation or other process to evaluate compliance with a specified set of security standards.

---

7 The term "Protected Health Information" does not appear in HIPAA's proposed security regulations. Instead, the term is defined in the final privacy regulations to include "individually identifiable health information" that has been transmitted or maintained electronically, or in any other medium. 45 C.F.R. 164.501, 65 F.R. 82805 (12/28/2000).
8 63 F. R. 43245 (8/12/98).
2. Chain of Trust Partner Agreement. Contracts entered into by two business entities where data is transmitted or exchanged and the sender and receiver agree to maintain the integrity and confidentiality of the data.


5. Information Access Controls. Formal policies/procedures for granting different levels of access to health information.

6. Internal Audits. In-house review of records of systems activity(e.g., logins).

7. Personnel Security. Policies to insure that persons with access have both authorization and proper clearances.

8. Security Configuration Management. Coordination and integration of security policies and practices to create a coherent system of security.


10. Security Management Process. Creation, administration and oversight of procedures to ensure the prevention, detection, containment, and correction of security breaches.

11. Termination Procedures. Formal process for ending a person’s employment and/or user access.

12. Training. Education of the vulnerability of health information and ways to ensure protection of the health information.

C. Security Standard Requirements for Physical Safeguards.


2. Media Controls. Policies to control the physical removal of hardware and or software form the secure environment/building.

3. Physical Access Controls. Controls for disaster recovery, emergency operation, maintenance of records, need to know procedures, sign-in, etc.
4. Policy and Guidelines on Workstation Use. Policies which delineate proper functions of a workstation and the manner in which they are performed.

5. Secure Workstation Location. Physical safeguards to limit unauthorized access to workstations.

6. Security Awareness Training. Training to imbed security into daily activities.


1. Access control including emergency access, use of encryption(optional).

2. Audit Controls. Mechanisms to record and examine system activity.

3. Authorization Controls. A mechanism for obtaining consent for use and disclosure of health information.

4. Data Authentication. Mechanisms to show that data has not been altered or destroyed in an unauthorized manner.

5. Entity Authentication. A mechanism by which an entity corroborates that is who it claims to be to prevent improper access(e.g., biometrics, passwords tokens).


Each organization that uses communications or networks would be required to protect communications containing health information that are transmitted electronically over open networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient, and to protect their information systems from intruders trying to access systems through external communication points.

When using open networks, some form of encryption should be employed. The utilization of less open systems/networks such as those provided by a value-added network (VAN) or private-wire arrangement provides sufficient access controls to allow encryption to be an optional feature. These controls would be important because of the potential for compromise of information over open
systems such as the Internet or dial-in lines. 63 Fed. Reg. 43255 (8/12/98). Requirements include:

1. Integrity Controls to ensure validity of messages.
2. Message Authentication to match what is sent to what is received.
3. Access Controls Over Network Communications.
4. Encryption of network messaging including alarm systems, audit trails, entity authentication and event reporting.

a. If an organization wishes to use an insecure transmission media such as the Internet, and take advantage of the low costs involved, offsetting costs may need to be incurred to provide for an acceptable form of encryption so that health information will be protected from intercept and possible misuse.

F. Documentation under the Security Regulations. In the aggregate, the proposed security regulations directly or indirectly will mandate development of an extensive array documents as follows.

1. Documents to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.
2. Chain of trust partner agreements
3. A contingency plan.
5. A disaster recovery plan.
6. A emergency mode operation plan.
7. Testing procedures for the contingency plan.
8. Policies that establish rules granting access.
9. Policies to determine types of, and reason to change access.
11. Maintaining records of access.
12. Policies assuring proper levels of access authorization.


14. Policies on appropriate clearances.

15. Procedures to coordinate and manage systems.


17. Formal instructions for reporting security incidents.


20. Sanction policies and procedures.

21. Security policy statements

22. Instructions on termination of employees.

23. Policies on changing locks.


25. A physical security plan.


27. Need to know procedures.

28. Policies on work station use.

29. Procedures for emergency access.

30. Procedures for audit trails.

G. Components of the Electronic Signature Standard.


There is no requirement to use electronic signatures in any mandated electronic transactions. If a user elects to use an electronic signature, it must meet the requirements of the standard.
2. Requirements of the Electronic signature Standard.

a. An electronic signature is the attribute affixed to an electronic message or document which binds it to a particular entity and secures user authentication.

b. An electronic signature must be a digital signature.

c. An electronic signature must ensure: message integrity; non-repudiation; and, user authentication.

H. Security—Privacy Overlap.

The proposed regulations on security and privacy suggest areas of overlap and mandates for which an enterprise will need to carefully coordinate its implementation activities. Obviously, the proposed privacy regulations define a universe of uses and disclosures which must be factored into the workings of a compliant security program.

The following concepts or requirements in the proposed security and the proposed privacy regulations seem to relate.

<table>
<thead>
<tr>
<th>Security</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chain of trust agreements</td>
<td>Business Associate agreements (&quot;BAKs&quot;)</td>
</tr>
<tr>
<td>Policies for dissemination</td>
<td>Minimum necessary limitation</td>
</tr>
<tr>
<td>Internal audits</td>
<td>Accounting procedures</td>
</tr>
<tr>
<td>Training</td>
<td>Training</td>
</tr>
<tr>
<td>Documentation</td>
<td>Documentation</td>
</tr>
<tr>
<td>Sanction policies</td>
<td>Sanction policies</td>
</tr>
<tr>
<td>Security incident reporting</td>
<td>BA reports of improper use</td>
</tr>
</tbody>
</table>
February 22, 2001

The Honorable Tommy G. Thompson
Secretary
U. S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, D.C. 20201

Dear Secretary Thompson:

As part of its responsibilities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the National Committee on Vital and Health Statistics (NCVHS) monitors the implementation of the Final Rules that adopt the health data standards required by the Administrative Simplification provisions of HIPAA.

The Final Rule for Standards for Electronic Transactions was published on August 17, 2000. The compliance date is October 16, 2002 (October 16, 2003 for small health plans). The health care industry is heavily involved in implementation activities in order to comply with the standards set forth in this Rule by the required dates. In the course of conducting these activities, the industry has encountered issues and concerns that need to be resolved as soon as possible to ensure timely compliance.

The Final Rule for Standards for Electronic Transactions adopted the National Drug Codes (NDCs) as the standard medical code set to be used to report drugs and biologics on standard transactions. While NDCs are currently used extensively on retail pharmacy claims, the requirement to use NDCs to report drugs on institutional and professional claims is new and is causing widespread concern within the health care industry. Today, the Health Care Financing Administration Common Procedure Coding System (HCPCS) drug codes are most widely used to report drugs and biologics on institutional and professional claims.

In a letter dated September 22, 2000, to former Secretary Donna Shalala, the National Uniform Billing Committee (NUBC) outlined its concerns with the requirement to use NDCs on institutional claims, particularly hospital claims. (The NUBC is named in HIPAA as an organization with which the Secretary must consult in adopting Administrative Simplification standards.) More recently, issues have been identified in change requests within the Designated Standard Maintenance Organization (DSMO) process. The DSMO process, described in the Final Rule in section 162.910, is the method by which standards are maintained and modified. The pending DSMO change requests ask to remove the requirement to use NDCs to report drugs and biologics on the standard institutional and professional claims.

On February 1, 2001, the Subcommittee on Standards and Security of the NCVHS held public hearings on HIPAA implementation issues. Health care industry representatives, including the NUBC chairman, presented testimony on concerns with the requirement to use NDCs. Those who testified and the organizations they represent support HIPAA and are deeply involved in HIPAA implementation activities. They and others from their organizations are members of most
of the health care industry workgroups that are carrying out this work. The concerns they identified are summarized below:

- Today, hospitals use NDCs for only two purposes: to purchase drugs and to maintain inventory control. NDCs serve these purposes well. NDCs are not used within hospitals to order drugs from the pharmacy, are not written into the patients’ medical records, and are not found in the patient accounting or billing systems. To comply with HIPAA, hospitals and other institutional providers would be required to conduct extensive conversions and replacement of existing information systems and interfaces. Staff would require training in the use of NDCs. There would be the potential for harm to patients as hospital pharmacies transition to NDCs. New interfaces with the dispensing systems that would need to be created could contain errors that may allow the wrong drug to be dispensed, resulting in a medication error. Hospitals routinely repackage drugs in convenient quantities, making the reporting of dosage more complex when NDCs need to be used. If a hospital pharmacy needs to furnish a substitute for a prescribed drug that is not on hand, it may be difficult to determine which drug should be dispensed when using NDCs because many NDCs can represent a single drug.

- Estimates indicate that the cost of moving to NDCs for reporting drugs and biologics on institutional claims could easily exceed an institution’s cost of adopting all the other transaction standards combined. While costs would vary depending on the size of the facility, hospitals estimate the minimum cost at $200,000 per facility to switch from using HCPCS codes to NDCs. Institutional providers would not benefit from the use of NDCs on claims and would incur high costs to convert.

- A recent survey of physician practices by a major designer of practice management systems indicated that HCPCS codes are used almost exclusively to report drugs and biologics. To comply with HIPAA, practice management systems used by providers would be required to expand fields in nearly all modules in order to store and display the thousands of NDCs. The industry estimates that typical physician practices spend as little as $800 to as much as $100,000 for their practice management systems. In general, practices with the most expensive systems would not want to spend more than about 10 percent of what they paid for a system to have that system made HIPAA compliant.

- Use of NDCs by providers to report drug dosages can be problematic. Drug packaging usually has the NDC printed on it. If one vial (from a box of ten) is used to administer injections to several patients, dosage reporting becomes complicated when using the NDC that is printed on the box that contained the ten vials. Calculations would need to be done to determine how much of the vial from the box of ten was used for a single injection, requiring the reporting of fractional units. This can be complicated and burdensome.

- Vendors’ product lines are directly impacted by the move from HCPCS codes to NDCs. Software packages that price drugs and that produce product dictionaries, screens, and reports would need to be changed.

- Two industry crosswalks or cross-references would need to be developed. One would crosswalk HCPCS drug codes to NDCs (one-to-many), and the other would do the
reverse (many-to-one). The crosswalks would be used for claims processing and drug pricing during the transition to NDCs. They would need to be updated quarterly to be consistent with the NDC code set updates. They would be needed right away in order to be able to use NDCs by the compliance date. In addition to educating the health care industry about the existence and use of the crosswalks, the costs of developing, maintaining, and disseminating them to the industry within the implementation period are concerns.

- Some industry representatives identified perceived deficiencies in the NDC maintenance process that they understood could result in re-use of NDCs and the possibility that an NDC for a particular drug could change over time. The Food and Drug Administration (FDA) indicated that it is attempting to resolve known deficiencies through the regulatory process. The FDA expressed its interest in making changes to the NDC code set to ultimately make it more useful to the health care industry in general.

- HHS staff testified that the comments received on the Proposed Rule touched upon some of the issues that were being discussed at the meeting, and more recent health care industry feedback has revealed significant problems being encountered in attempting to switch from using HCPCS drug codes to NDCs. HHS acknowledged that those problems warrant a more thorough investigation before a standard for drugs and biologics can be implemented in standard transactions other than for retail pharmacy.

Recommendations for HHS

It was clear that the industry strongly supports HIPAA and its administrative simplification provisions, and is working hard to implement the requirements of the Final Rule. In undertaking these efforts, however, many problems with the requirement to use NDCs to report drugs and biologics on the standard institutional and professional claims have become apparent. The problems described in testimony affect nearly all providers, health plans and health care clearinghouses and impede the ability of the health care industry to meet the HIPAA compliance date.

The NCVHS believes that further evaluation is needed before a standard code set for drugs and biologics can be implemented in standard transactions other than for retail pharmacy. We therefore recommend that the requirement at section 162.1002 (c) in the Final Rule for Standards for Electronic Transactions be modified by retracting the adoption of NDCs as the standard for drugs and biologics for use in standard transactions other than for retail pharmacy. We recommend that NDCs remain the standard for drugs and biologics in retail pharmacy transactions.

The NCVHS recommends that HHS work with ASC X12N to ensure that HCPCS codes as well as NDC codes can continue to be used in the standard institutional and professional claim transactions. The institutional and professional claim transactions should be able to accommodate NDCs in cases where those codes are useful or needed. (The ASC X12N dental claim does not capture drugs, so this issue does not affect that transaction standard.)

The NCVHS believes that no drug coding system in existence today fully meets the needs of the health care industry. HIPAA addresses drug coding primarily from a claims aspect, whereas the
future needs of the health care industry are for a drug coding system that can be used efficiently throughout the drug inventory, pharmacy, patient care, and billing arenas, and also used to ensure patient safety. The NCVHS recommends that HHS develop criteria that should be met by a drug coding system that could be useful throughout the health care industry, and evaluate any future proposed drug coding systems against those criteria.

We appreciate the opportunity to offer these comments and recommendations.

Sincerely,

John Lumpkin, M.D., M.P.H.

Chair
National Committee on Vital and Health Statistics
September 27, 2001

John Lumpkin, M.D., M.P.H.
Chair, National Committee on Vital and Health Statistics
6525 Belcrest Road
Room 1100
Hyattsville, MD 20782-2003

Dear Dr. Lumpkin:

Thank you for your letters regarding the implementation of the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). You raise many important issues, several of which are under active discussion at the Department of Health and Human Services (the Department).

We would like to respond to the specific recommendations in your letters. Because of the number of recommendations and our wish to be responsive to you in terms of current efforts at the Centers for Medicare & Medicaid Services and the Department, we have prepared an enclosure.

As always, we welcome your recommendations regarding implementation on HIPAA’s administrative simplification provisions. The National Provider Identifier final rule cannot be published until budget commitments for the costs of enumeration have been made, which we do not expect before FY 2003. As we continue implementation efforts, we look forward to working with the National Committee on Vital and Health Statistics.

Sincerely,

/ s /
Claude A. Allen
Deputy Secretary

Enclosure

RECOMMENDATIONS AND RESPONSES ON HIPPA IMPLEMENTATION

**Recommendation:**

Provide early guidance on new policies.

**Response:**

We have provided guidance on several occasions (including providing guidance on the privacy regulation and sending you a letter regarding our intention to publish a proposed rule revising the
drug coding standard) and will continue to do so whenever feasible. However, we are not able to provide information on final rules which are in the formal clearance process.

**Recommendation:**
Allow flexibility in the enforcement of the new standards.

**Response:**
The Department is planning to develop a regulation on enforcement of the HIPAA standards and will take your advice into consideration when we begin.

**Recommendation:**
Oppose delays in the compliance dates for the HIPAA standards such as those found in section 836.

**Response:**
We share your concern regarding the potential effects of delays. However, the Administration has taken no position on the pending legislation. We are proceeding with the compliance dates as stated in final regulations.

**Recommendation:**
Publish and implement HIPAA regulations quickly.

**Response:**
We recognize the need to issue these regulations as soon as possible. The Department is working toward publishing the final rule on security, and a proposed rule on a claims attachment standard, by the end of the year. The National Provider Identifier rule is currently under development.

**Recommendation:**
Expedite the HIPAA change process.

**Response:**
We are committed to working with designated standards maintenance organizations (DSMOs) in order to streamline the process and will work to publish the recommended changes in regulations as soon as possible.

**Recommendation:**
Explore consistent standards for paper transactions.
Response:

We will work through our Department representatives to the National Uniform Claim Committee and to the National Uniform Billing Committee to bring this issue to the attention of the Committee.

Recommendation:

Accept DMSO recommendations for changes to the standard electronic transactions and code sets.

Response:

The Department has already begun the development of the regulations necessary to adopt these changes and intends to publish them as quickly as possible. We are working toward publication of a final rule early in Calendar year 2002. In addition, in order to ease your concerns regarding the coverage of the standard code sets, we will monitor the efforts of code set maintainers to ensure they are meeting the needs of the health care industry.
An Act

To ensure that covered entities comply with the standards for electronic health care transactions and code sets adopted under part C of title XI of the Social Security Act, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the `Administrative Simplification Compliance Act'.

SEC. 2. EXTENSION OF DEADLINE FOR COVERED ENTITIES SUBMITTING COMPLIANCE PLANS.

(a) IN GENERAL-
(1) EXTENSION- Subject to paragraph (2), notwithstanding section 1175(b)(1)(A) of the Social Security Act (42 U.S.C. 1320d-4(b)(1)(A)) and section 162.900 of title 45, Code of Federal Regulations, a health care provider, health plan (other than a small health plan), or a health care clearinghouse shall not be considered to be in noncompliance with the applicable requirements of subparts I through R of part 162 of title 45, Code of Federal Regulations, before October 16, 2003.

(2) CONDITION- Paragraph (1) shall apply to a person described in such paragraph only if, before October 16, 2002, the person submits to the Secretary of Health and Human Services a plan of how the person will come into compliance with the requirements described in such paragraph not later than October 16, 2003. Such plan shall be a summary of the following:
   (A) An analysis reflecting the extent to which, and the reasons why, the person is not in compliance.
   (B) A budget, schedule, work plan, and implementation strategy for achieving compliance.
   (C) Whether the person plans to use or might use a contractor or other vendor to assist the person in achieving compliance.
   (D) A timeframe for testing that begins not later than April 16, 2003.

(3) ELECTRONIC SUBMISSION- Plans described in paragraph (2) may be submitted electronically.

(4) MODEL FORM- Not later than March 31, 2002, the Secretary of Health and Human Services shall promulgate a model form that persons may use in drafting a plan described in paragraph (2). The promulgation of such form shall be made
without regard to chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act').

(5) ANALYSIS OF PLANS; REPORTS ON SOLUTIONS-

(A) ANALYSIS OF PLANS-

(i) FURNISHING OF PLANS- Subject to subparagraph (D), the Secretary of Health and Human Services shall furnish the National Committee on Vital and Health Statistics with a sample of the plans submitted under paragraph (2) for analysis by such Committee.

(ii) ANALYSIS- The National Committee on Vital and Health Statistics shall analyze the sample of the plans furnished under clause (i).

(B) REPORTS ON SOLUTIONS- The National Committee on Vital and Health Statistics shall regularly publish, and widely disseminate to the public, reports containing effective solutions to compliance problems identified in the plans analyzed under subparagraph (A). Such reports shall not relate specifically to any one plan but shall be written for the purpose of assisting the maximum number of persons to come into compliance by addressing the most common or challenging problems encountered by persons submitting such plans.

(C) CONSULTATION- In carrying out this paragraph, the National Committee on Vital and Health Statistics shall consult with each organization--

(i) described in section 1172(c)(3)(B) of the Social Security Act (42 U.S.C. 1320d-1(c)(3)(B)); or

(ii) designated by the Secretary of Health and Human Services under section 162.910(a) of title 45, Code of Federal Regulations.

(D) PROTECTION OF CONFIDENTIAL INFORMATION-

(i) IN GENERAL- The Secretary of Health and Human Services shall ensure that any material provided under subparagraph (A) to the National Committee on Vital and Health Statistics or any organization described in subparagraph (C) is redacted so as to prevent the disclosure of any--

(I) trade secrets;

(II) commercial or financial information that is privileged or confidential; and

(III) other information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

(ii) CONSTRUCTION- Nothing in clause (i) shall be construed to affect the application of section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act'), including the exceptions from disclosure provided under subsection (b) of such section.

(6) ENFORCEMENT THROUGH EXCLUSION FROM PARTICIPATION IN MEDICARE-
(A) IN GENERAL- In the case of a person described in paragraph (1) who fails to submit a plan in accordance with paragraph (2), and who is not in compliance with the applicable requirements of subparts I through R of part 162 of title 45, Code of Federal Regulations, on or after October 16, 2002, the person may be excluded at the discretion of the Secretary of Health and Human Services from participation (including under part C or as a contractor under sections 1816, 1842, and 1893) in title XVIII of the Social Security Act (42 U.S.C. 1395 et seq.).

(B) PROCEDURE- The provisions of section 1128A of the Social Security Act (42 U.S.C. 1320a-7a) (other than the first and second sentences of subsection (a) and subsection (b)) shall apply to an exclusion under this paragraph in the same manner as such provisions apply with respect to an exclusion or proceeding under section 1128A(a) of such Act.

(C) CONSTRUCTION- The availability of an exclusion under this paragraph shall not be construed to affect the imposition of penalties under section 1176 of the Social Security Act (42 U.S.C. 1320d-5).

(D) NONAPPLICABILITY TO COMPLYING PERSONS- The exclusion under subparagraph (A) shall not apply to a person who--

(i) submits a plan in accordance with paragraph (2); or

(ii) who is in compliance with the applicable requirements of subparts I through R of part 162 of title 45, Code of Federal Regulations, on or before October 16, 2002.

(b) SPECIAL RULES-

(1) RULES OF CONSTRUCTION- Nothing in this section shall be construed--

(A) as modifying the October 16, 2003, deadline for a small health plan to comply with the requirements of subparts I through R of part 162 of title 45, Code of Federal Regulations; or

(B) as modifying--

(i) the April 14, 2003, deadline for a health care provider, a health plan (other than a small health plan), or a health care clearinghouse to comply with the requirements of subpart E of part 164 of title 45, Code of Federal Regulations; or

(ii) the April 14, 2004, deadline for a small health plan to comply with the requirements of such subpart.

(2) APPLICABILITY OF PRIVACY STANDARDS BEFORE COMPLIANCE DEADLINE FOR INFORMATION TRANSACTION STANDARDS-

(A) IN GENERAL- Notwithstanding any other provision of law, during the period that begins on April 14, 2003, and ends on October 16, 2003, a health care provider or, subject to subparagraph (B), a health care clearinghouse, that transmits any health information in electronic form in connection with a transaction described in subparagraph (C) shall comply with the requirements of subpart E of part 164 of title 45, Code of Federal Regulations, without regard to whether the transmission meets the standards required by part 162 of such title.

(B) APPLICATION TO HEALTH CARE CLEARINGHOUSES- For purposes of this paragraph, during the period described in subparagraph
(A), an entity that processes or facilitates the processing of information in connection with a transaction described in subparagraph (C) and that otherwise would be treated as a health care clearinghouse shall be treated as a health care clearinghouse without regard to whether the processing or facilitation produces (or is required to produce) standard data elements or a standard transaction as required by part 162 of title 45, Code of Federal Regulations.

(C) TRANSACTIONS DESCRIBED- The transactions described in this subparagraph are the following:

(i) A health care claims or equivalent encounter information transaction.
(ii) A health care payment and remittance advice transaction.
(iii) A coordination of benefits transaction.
(iv) A health care claim status transaction.
(v) An enrollment and disenrollment in a health plan transaction.
(vi) An eligibility for a health plan transaction.
(vii) A health plan premium payments transaction.
(viii) A referral certification and authorization transaction.

(c) DEFINITIONS- In this section--

(1) the terms `health care provider', `health plan', and `health care clearinghouse' have the meaning given those terms in section 1171 of the Social Security Act (42 U.S.C. 1320d) and section 160.103 of title 45, Code of Federal Regulations;
(2) the terms `small health plan' and `transaction' have the meaning given those terms in section 160.103 of title 45, Code of Federal Regulations; and
(3) the terms `health care claims or equivalent encounter information transaction', `health care payment and remittance advice transaction', `coordination of benefits transaction', `health care claim status transaction', `enrollment and disenrollment in a health plan transaction', `eligibility for a health plan transaction', `health plan premium payments transaction', and `referral certification and authorization transaction' have the meanings given those terms in sections 162.1101, 162.1601, 162.1801, 162.1401, 162.1501, 162.1201, 162.1701, and 162.1301 of title 45, Code of Federal Regulations, respectively.

SEC. 3. REQUIRING ELECTRONIC SUBMISSION OF MEDICARE CLAIMS.

(a) IN GENERAL- Section 1862 of the Social Security Act (42 U.S.C. 1395y) is amended--

(1) in subsection (a)--

(A) by striking `or' at the end of paragraph (20);
(B) by striking the period at the end of paragraph (21) and inserting `; or'; and
(C) by inserting after paragraph (21) the following new paragraph:

`(22) subject to subsection (h), for which a claim is submitted other than in an electronic form specified by the Secretary.'; and

(2) by inserting after subsection (g) the following new subsection:

`(h)(1) The Secretary--

`(A) shall waive the application of subsection (a)(22) in cases in which--
(i) there is no method available for the submission of claims in an electronic form; or
(ii) the entity submitting the claim is a small provider of services or supplier; and
(B) may waive the application of such subsection in such unusual cases as the Secretary finds appropriate.
(2) For purposes of this subsection, the term `small provider of services or supplier’ means--
(A) a provider of services with fewer than 25 full-time equivalent employees; or
(B) a physician, practitioner, facility, or supplier (other than provider of services) with fewer than 10 full-time equivalent employees.
(b) EFFECTIVE DATE- The amendments made by subsection (a) shall apply to claims submitted on or after October 16, 2003.

SEC. 4. CLARIFICATION WITH RESPECT TO APPLICABILITY OF ADMINISTRATIVE SIMPLIFICATION REQUIREMENTS TO MEDICARE+CHOICE ORGANIZATIONS.

Section 1171(5)(D) of the Social Security Act (42 U.S.C. 1320d(5)(D)) is amended by striking `Part A or part B’ and inserting `Parts A, B, or C’.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS FOR IMPLEMENTATION OF REGULATIONS.

(a) IN GENERAL- Subject to subsection (b), and in addition to any other amounts that may be authorized to be appropriated, there are authorized to be appropriated a total of $44,200,000, for--
(1) technical assistance, education and outreach, and enforcement activities related to subparts I through R of part 162 of title 45, Code of Federal Regulations; and
(2) adopting the standards required to be adopted under section 1173 of the Social Security Act (42 U.S.C. 1320d-2).

(b) REDUCTIONS-
(1) MODEL FORM 14 DAYS LATE- If the Secretary fails to promulgate the model form described in section 1(a)(4) by the date that is 14 days after the deadline described in such section, the amount referred to in subsection (a) shall be reduced by 25 percent.
(2) MODEL FORM 30 DAYS LATE- If the Secretary fails to promulgate the model form described in section 1(a)(4) by the date that is 30 days after the deadline described in such section, the amount referred to in subsection (a) shall be reduced by 50 percent.
(3) MODEL FORM 45 DAYS LATE- If the Secretary fails to promulgate the model form described in section 1(a)(4) by the date that is 45 days after the deadline described in such section, the amount referred to in subsection (a) shall be reduced by 75 percent.
(4) MODEL FORM 60 DAYS LATE- If the Secretary fails to promulgate the model form described in section 1(a)(4) by the date that is 60 days after the deadline described in such section, the amount referred to in subsection (a) shall be reduced by 100 percent.
Speaker of the House of Representatives.
Vice President of the United States and
President of the Senate.
HIPAA Administrative Simplification Compliance Act (ASCA)
Frequently Asked Questions

Q1: What will be the impact of the one-year extension?
A1: The delay will give covered entities more time to build, test, and successfully implement the new Final Electronic Transactions and Code Sets required by HIPAA.

Q2: Does the extension affect the compliance date for the HIPAA privacy standards?
A2: No, the compliance date for the privacy standards is still April, 2003 or, for small health plans, April 2004.

Q3: Can small health plans get an extension to their current compliance date of October, 2003?
A3: No, the compliance date for small plans does not change.

Q4: Do all covered entities automatically get an extension?
A4: No. Covered entities must submit a compliance extension plan to the Department of Health and Human Services (HHS) before October 16, 2002 to get an extension.

Q5: Why didn’t Congress just give everyone an extension?
A5: The requirement to submit a compliance extension plan provides assurance that covered entities have plans in place that will allow them to be compliant by the new deadline of October 16, 2003.

Q6: Is HHS going to actually review and approve all these compliance extension plans? Will some be denied?
A6: The law does not require approval or disapproval of plans. Submission of an extension plan is sufficient to secure the one-year extension.

Q7: When will the model compliance extension form be available?
A7: The form will be available by March 31, 2002.

Q8: Where can I get a copy of the form? Do I have to use the form, or can I submit a compliance plan in another format?
A8: We will publish the form in the Federal Register and will also make it available on several websites. The compliance extension form we are developing is a model. While we strongly recommend its use, covered entities may submit plans using other formats.

Q9: How extensive will the model compliance extension form be?
A9: We are still working on the form, but we intend to make it as simple and easy to complete as possible. The ASCA requires the plans to contain summary information regarding compliance activities, including: 1) budget, schedule, work plan and implementation strategy for achieving compliance; 2) planned use of contractors or vendors; 3) assessment of compliance problems; and 4) a timeframe for testing to begin no later than April 16, 2003.

Q10: My organization has a very detailed, voluminous compliance plan – are we supposed to submit the whole thing?
A10: No. The compliance extension form will ask only for summary information from your detailed plan. You do not need to send other information.

Q11: Can I file the compliance extension form electronically?
A11: Yes, we will encourage electronic filing of compliance extension plans, although we will also accept plans submitted on paper.

Q12. What will be the application deadline for a delay?
A12. Covered entities must submit their compliance extension plans by October 15, 2002.

Q13: Where should I send my completed compliance extension form?
Q13: Please do not submit requests at this time. Instructions will be issued that will explain how to submit compliance extension plans.

Q14: How will one covered entity know whether another covered entity with which it does business has submitted a plan?
A14: Each covered entity should communicate directly with its own trading partners to determine which ones have submitted plans. This information could be included in establishing schedules for the testing activities that are to begin by April 16, 2003, culminating in a migration to the new standards that meets the needs of all trading partners.

Q15: I believe I will be fully compliant by October, 2002. However, I know that some of my trading partners are requesting extensions and will continue to use nonstandard formats after that date. Do I need to submit a compliance extension plan so that I can continue to communicate with these partners using nonstandard transactions?
A15: No. A covered entity will be considered compliant if it can send and receive compliant transactions, and therefore would not need to submit an extension plan.

Q16: Can a plan require its network providers to move to standard transactions before October 16, 2003?
A16: This is a business decision between the plan and its provider network. Neither HIPAA nor ASCA preclude plans from requiring that their providers use standard transactions in advance of the compliance deadline, but HIPAA non-compliance penalties would not apply to a provider that has submitted a plan until 2003.

Q17: What will be done with the information I provide?
A17: ASCA requires that a sample of the plans will be provided to the National Committee on Vital and Health Statistics (NCVHS), an advisory committee to the Secretary of Health and
Human Services. The NCVHS will review the sample to identify common problems that are complicating compliance activities, and will periodically publish recommendations for solving the problems.

Q18: Will the information I provide be made public?
A18: Under the Freedom of Information Act (FOIA), information held by the federal government is available to the public on request, unless it falls within one of several exemptions. The model form will be designed to avoid collection of any information that would be subject to exemption, such as confidential personal or proprietary information. If such information is submitted, both the FOIA and the ASCA require that it be redacted before the files are released either to the NCVHS or to the public.

Q19: How does the delay affect Medicare implementation activities?
A19: Medicare will continue to implement the HIPAA transaction standards on a sequenced basis, and that schedule will not change significantly. We expect to be ready to test the claim and several other transactions by Spring 2002, but implementation of several transactions (such as the referral/authorization transaction) will be in early FY 2003. Once a provider has successfully tested a transaction with us, it will be able to use the standard in our production environment.

Q20: When will Medicaid Agencies begin testing compliant transactions with their trading partners?
A20: Each Medicaid State Agency has its own project plan for achieving HIPAA compliance, and will decide whether to submit a compliance extension plan. If you are a trading partner, you will receive notice of testing directly from the Medicaid State Agency(s) with whom you do business.

Q21: Do software vendors need to file for an extension?
A21: No. Only covered entities – plans, clearinghouses and providers – must file. In fact, vendors will need to maintain their current delivery schedules for compliant software in order for covered entities to make use of the additional implementation time.

Q22: Should covered entities discontinue testing until 2003?
A22: ASCA requires that compliance plans include a testing phase that would begin no later than April 16, 2003. We recommend that all covered entities begin to test as soon as they are ready in order to allow adequate time to address and correct problems. CMS will soon send out an instruction with dates by which Medicare contractors must begin testing with providers.

Q23: ASCA allows the Secretary of HHS to exclude covered entities from the Medicare program if they do not submit a compliance extension plan or achieve compliance by October, 2002. Will every such covered entity be excluded?
A23: HHS will be publishing proposed regulations to address this new exclusion authority.

Q24: Doesn’t the law also require Medicare claims to be submitted electronically after October, 2003?
A24: ASCA prohibits HHS from paying Medicare claims that are not submitted electronically after October 16, 2003, unless the Secretary grants a waiver from this requirement. It further provides that the Secretary must grant such a waiver if there is no method available for the submission of claims in electronic form or if the entity submitting the claim is a small provider of services or supplies. Beneficiaries will also be able to continue to file paper claims if they need to file a claim on their own behalf. The Secretary may grant such a waiver in other circumstances. We will publish proposed regulations to implement this new authority.