HIPAA Frequently Asked Questions

GENERAL

1. What is HIPAA?
2. Who must comply with HIPAA?
3. Since the regulations frequently refer to "electronic" communication, what media falls into that category?
4. When do organizations have to comply with the standards?
5. Is there any consideration for small plans for complying with the standard once it is adopted?
6. How is a small plan defined?
7. Does a Health Plan have to accept transactions?
8. Can health plans delay payments for transactions submitted electronically according to the standard?
9. I am an employer and I provide on site healthcare for my employees. Do these HIPAA standards apply to me?
10. I am an employer and I do not provide on site healthcare for my employees. Do these HIPAA standards apply to me?
11. Is HIPAA a way for the government to create one large database with everyone's health information?
12. I am a physician. I do not own a computer. Do I have to buy a computer?
13. Why all the DHHS delays in publishing the final HIPAA regulations?
14. How does one become a HIPAA accredited agency?

CODE SET STANDARDS

1. What is a code set?
2. What code sets have been adopted as HIPAA standards?
3. Can HCPCS Level 3 codes established on a local basis still be used?
4. Where can I get more information about the code sets?

ELECTRONIC TRANSACTION STANDARDS

1. Why have national standards for electronic health care transactions been adopted? Why are they required?
2. What health care transactions are required to use the standards under this regulation?
3. Who is required to use the standards?
4. If a health plan does not perform a transaction electronically, must it implement the standard?
5. When will the standards become effective?
6. Where did these standards come from? Did the Federal Government create them?
7. What standards were chosen?
8. Do these standards apply to transactions sent over the Internet?
9. Do I have to use standard transactions when conducting business inside my corporate boundaries?
10. What is the effect of these standards on State law?
11. Are any exceptions allowed?
12. What does the law require of State Medicaid programs?
13. How will the standards be enforced?
14. How were the standards chosen?
15. Where can I obtain implementation guides for the standards?
16. How can the standards be changed?
17. Does the law require physicians to buy computers?
18. How will the standards affect data stored in my system?
19. Can health plans require changes or additions to the standard claim?

20. Should health plans publish companion documents that augment the information in the standard implementation guides for electronic transactions?
21. Could companion documents from health plans define cases where the health plan wants particular pieces of data used or not used?
22. May health plans stipulate the codes or data values they are willing to accept and process in order to simplify implementation?
23. May health plans stipulate the number of loop iterations or the file sizes they are willing to accept?

PRIVACY STANDARDS

1. What about faxed transmissions?
2. On a call back to the patient to remind them of their appointment, if there is no answer, can we leave a message on their answering machine as to when their next appointment is?
3. Is there a federal privacy protection today?
4. Is this privacy protection consistent across the States?
5. How much of my personal information is going to be released?
6. What does the Privacy Standard provide?
7. Who can use my health information?
8. Can my information be used for other uses such as hospital fund raising or marketing?
9. Is there any assurance that my information has not been released if I do not sign an individual authorization?
10. I want to review my recent hospitalization records. Can I do that?

SECURITY AND ELECTRONIC SIGNATURES

1. Why are there standards for Security and Electronic Signature?
2. Why is there a need for standards for Security and Electronic Signature?
3. What are the main requirements of the Security Standards?
4. How will the Security Standards solve problems?
5. How will the Electronic Signature Standard solve problems?
6. Who must comply with the Security Standards?
7. Who must comply with the Electronic Signature Standard?
8. We are not currently using an electronic signature. Do I have to initiate this project?
9. Do the Security Standards apply just to transactions covered by HIPAA as the Electronic Signature Standards do?
10. What about hard copies of individual health information?
11. Does the Security Standard specify a technology to be used?
12. How do the standards affect all the data that is stored in my system?

UNIQUE IDENTIFIERS

1. Why is a Standard for an Employer Identifier Number (EIN) needed?
2. What number is being proposed for the EIN?
3. Do all employers have this taxpayer identifying number?
4. Don't some employers have more than one taxpayer identifying number?
5. Which taxpayer identifying number (EIN) are they to use if they have more than one?
6. Who is responsible for using the EIN?
7. What is the National Provider Identifier (NPI)?
8. Who would be given an NPI?
9. Who are considered health care providers?
10. Who are not considered health care providers?
11. How will NPIs be issued?
12. Who or what are "enumerators?"
13. How would Option 1 work?
14. How would Option 2 work?
15. How will NPIs be used?

16. Currently, Unique Physician Identifier Number (UPIN) exists in the Medicare program for identification. Will there be any relationship between UPIN and NPI?
17. Will foreign health care providers be assigned an NPI?
18. Is there a difference between the PlanID and the NPI or are they the same?
19. What is the difference between the health plan identifier (PAYERID) and PlanID?
20. What is a Unique Identifier for Individuals?
21. What is happening with the Individual Identifier? Will we have one or not?
22. Why would an Individual Identifier be needed?
23. Everyone has a Social Security Number, why not use that as the unique identifier?

ADMINISTRATIVE SIMPLICIFICATION COMPLIANCE ACT

1. What is the HIPAA Administrative Simplification Compliance Act (ASCA)?
2. Where can I get a copy of the ASCA compliance form?
3. Is my organization supposed to submit our entire detailed compliance plan?
4. Does the law require Medicare claims to be submitted electronically after Oct. 2003?
5. What will be the impact of the one-year ASCA extension?
6. How extensive will the model ASCA compliance extension form be?
7. Do software vendors need to file for an ASCA extension?
8. Is HHS going to actually review & approve all ASCA compliance plans?
9. Can I file the ASCA compliance extension form electronically?
10. Does the ASCA extension affect the compliance date for the HIPAA privacy standards?
11. Do all covered entities automatically get an ASCA extension?
12. Why didn't Congress just give everyone an ASCA extension?
13. Will noncompliant covered entities that fail to file an ASCA compliance plan be excluded from Medicare?
14. Will some ASCA compliance plans be denied?
15. Do I have to use the ASCA form?
16. How does the ASCA delay affect Medicare implementation activities?
17. When will Medicaid Agencies test ASCA compliant transactions with trading partners?
18. Should covered entities discontinue testing until 2003?
19. Where should I send my completed ASCA compliance form?
20. Can small health plans get an ASCA extension to their current compliance date?
21. Must I file an ASCA compliance plan to communicate with noncompliant partners?
22. How will an entity know if another entity has filed an ASCA compliance plan?
23. How does the delay affect Medicare implementation activities?
24. Can plans make network providers move to standard transactions before 10/16/03?

GENERAL

1. What is HIPAA

HIPAA, the Health Insurance Portability and Accountability Act of 1996 mandates standards for electronic data interchange (EDI) and code sets, establishes uniform health care identifiers, and seeks protections for confidentiality and security of patient data.

2. Who must comply with HIPAA?

All healthcare providers, health plans, payers, clearinghouses, and other entities that process health data must comply.

Any healthcare provider that electronically sends one of the transactions covered in the Final Rules (Claims, remittances, claim status inquiries, eligibility, certification) is covered by HIPAA. Any organization that electronically stores or transmits individually identified healthcare information must comply with the Security regulation. So, if the organization does any of the above (file a claim electronically or electronically store any healthcare info that can be tracked back to an individual) they must comply with the appropriate HIPAA regulation

3. Since the regulations frequently refer to "electronic" communication, what media falls into that category?

HIPAA applies to all communication that is stored or transmitted electronically, or that has been stored or transmitted electronically in the past. Media includes, but is not limited to, computer databases, tapes, disks, telecommunications, FAX, Internet, networks.

4. When do organizations have to comply with the standards?

Organizations have 24 months to comply with the Standard after the Standard is adopted.

5. Is there any consideration for small plans for complying with the standard once it is adopted?

Yes. Small plans will have 36 months to comply after the standard is adopted.

6. How is a small plan defined?

A small plan is one that meets the definition of a small business, under the Small Business Association's rules, annual receipts of less than $5 million.

7. Does a Health Plan have to accept transactions?

Health Plans may not refuse to accept standard transactions that are submitted electronically.

8. Can health plans delay payments for transactions submitted electronically according to the standard?

There will be no delay of payments by the health plans because the transactions are submitted electronically in compliance with the standards.

9. I am an employer and I provide on site healthcare for my employees. Do these HIPAA standards apply to me?

Yes. When an employer acts in the role of a health plan or health care provider, the employer must comply with HIPAA standards.

10. **I am an employer and I do not provide on site healthcare for my employees. Do these HIPAA standards apply to me?**

    No. The HIPAA standards do not apply to you as an employer since you do not act in the role of a health plan or health care provider. Employers can voluntarily choose to use HIPAA standard transactions to expedite their health plan activities, such as enrollment.

11. **Is HIPAA a way for the government to create one large database with everyone's health information?**

    There is no provision in HIPAA law to create, or propose to create, such a database. HIPAA is designed to reduce cost and administrative burden. HIPAA recognized the significance of protecting personal health information. New security standards and more privacy legislation are intended to protect the confidentiality of health care information.

12. **I am a physician. I do not own a computer. Do I have to buy a computer?**

    There is no requirement under HIPAA that you must own a computer. However, you may want to use a computer when you submit and receive transactions. In the future, this is likely to become the standard means for managing healthcare business.

13. **Why all the DHHS delays in publishing the final HIPAA regulations?**

    Once a proposed rule is approved by the government, the public is given the opportunity to comment on the proposal, and those comments must be considered in development of the final rules. Most of the proposed HIPAA regulations generated thousands of public comments, and the time required to review and consider them has slowed the publication of final rules.

14. **How does one become a HIPAA accredited agency?**

    There is really no such thing as becoming a HIPAA accredited agency. There is no agency at present, or, based on my knowledge, in the future, that will assume the role of accrediting an organization. On a side note, the healthcare industry at this point is very negative against any vendor who says they are HIPAA compliant. Their negative reaction is based on a number of reasons, 1) The majority of the rules are not yet final, 2) becoming HIPAA compliant requires a concerted effort from all parties, including the actual organization, its vendors, and its business associates.

CODE SET STANDARDS

1. What is a code set?

Under HIPAA, a "code set" is any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnosis codes, or medical procedure codes. Medical data code sets used in the health care industry include coding systems for diseases, impairments, other health related problems, and their manifestations; causes of injury, disease, impairment, or other health-related problems; actions taken to prevent, diagnose, treat, or manage diseases, injuries, and impairments; and any substances, equipment, supplies, or other items used to perform these actions. Code sets for medical data are required for data elements in the administrative and financial health care transaction standards adopted under HIPAA for diagnoses, procedures, and drugs.

2. What code sets have been adopted as HIPAA standards?

International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2 (including The Official ICD-9-CM Guidelines for Coding and Reporting), as updated and distributed by HHS, for the following conditions:

1. Diseases.
2. Injuries.
3. Impairments.
4. Other health related problems and their manifestations.
5. Causes of injury, disease, impairment, or other health-related problems.

International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volume 3 Procedures (including The Official ICD-9-CM Guidelines for Coding and Reporting), as updated and distributed by HHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals:

1. Prevention.
2. Diagnosis.
3. Treatment.
4. Management.

National Drug Codes (NDC), as updated and distributed by HHS, in collaboration with drug manufacturers, for the following:

1. Drugs.
2. Biologics.

Code on Dental Procedures and Nomenclature, as updated and distributed by the American Dental Association, for dental services.

The combination of **Health Care Financing Administration Common Procedure Coding System (HCPCS)**, as updated and distributed by HHS; and **Current Procedural Terminology, Fourth Edition (CPT-4)**, as updated and distributed by the American Medical Association, for physician services and other health related services. These services include, but are not limited to, the following:

1. Physician services.
2. Physical and occupational therapy services.
3. Radiological procedures.
4. Clinical laboratory tests.
5. Other medical diagnostic procedures.

6. Hearing and vision services.
7. Transportation services including ambulance.

The **Health Care Financing Administration Common Procedure Coding System (HCPCS)**, as updated and distributed by HCFA, HHS, for all other substances, equipment, supplies, or other items used in health care services. These items include, but are not limited to, the following:

1. Medical supplies.
2. Orthotic and prosthetic devices.
3. Durable medical equipment.

3. Can HCPCS Level 3 codes established on a local basis still be used?

No. All local codes will be eliminated. Users that need codes must apply to the appropriate organizations (e.g. HCFA for HCPCS codes, the AMA for CPT-4 codes) for national codes.

4. Where can I get more information about the code sets?

ICD-9-CM: Official version is available on CD-ROM from the Government Printing Office (GPO) at 202-512-1800 or FAX: 202-512-2250. The CD-ROM contains the ICD-9-CM classification and coding guidelines. Versions of ICD-9-CM are also available from several private sector vendors.

CPT-4: Official version is available from the American Medical Association. Versions are also available from several private sector vendors.

HCPCS: Information about HCPCS is available from the HCFA web site at http://www.hcfa.gov/medicare/hcpcs.htm.

Code on Dental Procedures and Nomenclature: Official version is available from the American Dental Association at 800-947-4746.

NDC: Official versions of the files are available on the Internet at http://www.fda.gov/cder/ndc/index.htm. NDC codes are also published in the Physicians' Desk Reference under the individual drug product listings and "How supplied." The supplements are available quarterly on diskette from the National Technical Information Service at 703-487-6430.

ELECTRONIC TRANSACTION STANDARDS

1. Why have national standards for electronic health care transactions been adopted? Why are they required?

Congress and the health care industry have agreed that standards for the electronic exchange of administrative and financial health care transactions are needed to improve the efficiency and effectiveness of the health care system. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of Health and Human Services to adopt such standards.

National standards for electronic health care transactions will encourage electronic commerce in the health care industry and ultimately simplify the processes involved. This will result in savings from the reduction in administrative burdens on health care providers and health plans. Today, health care providers and health plans that conduct business electronically must use many different formats for electronic transactions. For example, about 400 different formats exist today for health care claims. With a national standard for electronic claims and other transactions, health care providers will be able to submit the same transaction to any health plan in the United States and the health plan must accept it. Health plans will be able to send standard electronic transactions such as remittance advices and referral authorizations to health care providers. These national standards will make electronic data interchange a viable and preferable alternative to paper processing for providers and health plans alike.

2. What health care transactions are required to use the standards under this regulation?

As required by HIPAA, the Secretary of Health and Human Services is adopting standards for the following administrative and financial health care transactions:

1. Health claims and equivalent encounter information.
2. Enrollment and disenrollment in a health plan.
3. Eligibility for a health plan.
4. Health care payment and remittance advice.
5. Health plan premium payments.
6. Health claim status.
7. Referral certification and authorization.
8. Coordination of benefits.

Standards for the first report of injury and claims attachments (also required by HIPAA) will be adopted at a later date.

3. Who is required to use the standards?

All private sector health plans (including managed care organizations and ERISA plans, but excluding certain small self administered health plans) and government health plans (including Medicare, State Medicaid programs, the Military Health System for active duty and civilian personnel, the Veterans Health Administration, and Indian Health Service programs), all health care clearinghouses, and all health care providers that choose to submit or receive these transactions electronically are required to use these standards. These "covered entities" must use the standards when conducting any of the defined transactions covered under the HIPAA.

A health care clearinghouse may accept nonstandard transactions for the sole purpose of translating them into standard transactions for sending customers and may accept standard transactions and translate them into nonstandard transactions for receiving customers.

4. If a health plan does not perform a transaction electronically, must it implement the standard?

If the plan performs that business function (whether electronically, on paper, via phone, etc.), it must be able to support the electronic standard for that transaction. It may do this directly or through a clearinghouse.

5. When will the standards become effective?

All health plans, all health care clearinghouses, and any health care provider that chooses to transmit any of the transactions in electronic form must comply within 24 months after the effective date of the final rule (small health plans have 36 months). The effective date of the rule is 2 months after publication. Therefore, compliance with the final rule is required by October 2002 (October 2003 for small health plans). Entities can begin using these standards earlier than the compliance date.

6. Where did these standards come from? Did the Federal Government create them?

HIPAA required the Secretary to adopt standards, when possible, that have been developed by private sector standards development organizations (SDOs) accredited by the American National Standards Institute (ANSI). These are not government agencies. All of the transactions adopted by this rule are from such organizations. All are from the Accredited Standards Committee (ASC) X12N except the standards for retail pharmacy transactions, which are from the National Council for Prescription Drug Programs (NCPDP).

7. What standards were chosen?

ANSI ASC X12N standards, Version 4010, were chosen for all of the transactions except retail pharmacy transactions. The choice for the retail pharmacy transactions was the standard maintained by the NCPDP because it is already in widespread use. The NCPDP Telecommunications Standard Format Version 5.1 and equivalent NCPDP Batch Standard Version 1.0 have been adopted in this rule (health plans will be required to support one of these two NCPDP formats).

8. Do these standards apply to transactions sent over the Internet?

Internet transactions are being treated the same as other electronic transactions. However, we recognize that there are certain transmission modes in which the format portion of the standard is inappropriate. In these cases, the transaction must conform to the data content portion of the standard. In particular, a "direct data entry" process, where the data are directly keyed by a health care provider into a health plan's computer using dumb terminals or computer browser screens, would not have to use the format portion of the standard, but the data content must conform. If the data are directly entered into a system that is outside the health plan's system, to be transmitted later to the health plan, the transaction must be sent using the format and content of the standard.

9. Do I have to use standard transactions when conducting business inside my corporate boundaries?

The decision on when a standard must be used does not depend on whether the transaction is being sent inside or outside corporate boundaries. Instead, a simple two part test, in question form, can be used to determine whether the standards are required.

> **Question 1:** Is the transaction initiated by a covered entity or its business associate? If no, the standard need not be used.
>
> **Question 2:** Is the transaction one for which the Secretary had adopted a standard? If yes, the standard must be used. If no, the standard need not be used.

For purposes of question 1, a business associate acting on behalf of a covered entity can only perform those particular functions that the covered entity itself could perform in the transaction. The regulation requires health plans to accept standard transactions from any person.

For purposed of question 2, the definitions of the transactions themselves, as stipulated in Subpart K through Subpart R of the regulation, must be used to determine if the function is a transaction for which the Secretary has adopted a standard.

10. What is the effect on State law?

Section 1178 of the Social Security Act provides that standards for the transactions will supersede any State law that is contrary to them, but allows for an exception process. This process is currently under development and will be issued in the final rule for Privacy Standards.

11. Are any exceptions allowed?

In addition to the exceptions for conflicting State laws, an exception may be allowed for the testing of proposed modifications to the standards. An entity wishing to test a different standard may apply for an exception to test the new standard. Instructions for applications are published in the final rule. In this way, we hope to encourage the development of new technologies.

12. What does the law require of state Medicaid programs?

Section 1171(5)(E) of the Social Security Act, as enacted by HIPAA, identifies the State Medicaid programs as health plans, which therefore must be capable of receiving, processing, and sending standard transactions electronically. There is no requirement that internal information systems maintain data in accordance with the standards. However, Medicaid programs will need the capacity to process standard claim, encounter, enrollment, eligibility, remittance advice, and other transactions. In addition, as health plans, the State Medicaid programs will be required to comply with other HIPAA standards two years after adoption of the standards.

The standards should benefit Medicaid programs in multiple areas. Here are a few examples:

- A national standard for encounter transactions will provide a much-needed method for collecting encounter data on Medicaid beneficiaries enrolled in managed care. Because of the standards, it will be possible to combine encounter data from managed care with similar claims data from fee-for-service, thus enhancing the ability to monitor utilization, costs, and quality of care in managed care and to compare managed care with fee-for-service.
- The standard transactions will include methods for electronic exchange of enrollment information between the Medicaid program and private managed care plans enrolling Medicaid beneficiaries. This will reduce administrative costs of exchanging such information and enhance the reliability of such information.
- The conversion to national standards provides an opportunity for Medicaid programs to shift to commercial software or clearinghouses and to stop the expensive maintenance of old, customized transaction systems.

13. How will the standards be enforced?

The law gives the Secretary the authority to impose monetary penalties for failure to comply with a standard. The Secretary is required by statute to impose penalties of not more than $100 per violation on any person or entity who fails to comply with a standard except that the total amount imposed on any one person in each calendar year may not exceed $25,000 for violations of one requirement. Enforcement procedures will be published in a future regulation.

14. How were the standards chosen?

First, the Department developed a set of guiding principles to serve as the basis for evaluating alternative standards for each transaction. These guiding principles, designed to be consistent with the intent of HIPAA, are published in the regulation. Second, an inventory of standards was developed by the ANSI Health Informatics Standards Board, a private sector organization. Third, teams composed of representatives from several government agencies evaluated the available standards against the guiding principles to determine which standards best met the principles. Extensive outreach and consultation, including public meetings, with all facets of the health care industry continued throughout this process.

As required by HIPAA, the Secretary also consulted with the National Uniform Claim Committee (NUCC), the National Uniform Billing Committee (NUBC), the American Dental Association (ADA), and the Workgroup for Electronic Data Interchange (WEDI). The Secretary also considered advice from the National Committee on Vital and Health Statistics (NCVHS) and representatives of the health care industry who testified before the NCVHS Subcommittee on Health Data Needs, Standards, and Security.

Data dictionaries are available for an additional fee.

15. Where can I obtain implementation guides for the standards?

The implementation guides for the ASC X12N standards may be obtained from the Washington Publishing Company, 806 W. Diamond Ave., Suite 400, Gaithersburg, MD, 20878; telephone: 301-949-9740; FAX: 301-949-9742. These guides are also available at no cost through the Washington Publishing Company on the Internet at http://www.wpc-edi.com/hipaa/.

The implementation guide for retail pharmacy standards is available from the National Council for Prescription Drug Programs, 4201 North 24th Street, Suite 365, Phoenix, AZ, 85016; telephone: 602-957-9105; FAX: 602-955-0749. It is also available from the NCPDP's web site at http://www.ncpdp.org/.

16. How can the standards be changed?

The Secretary has designated six organizations that have agreed to serve as Designated Standards Maintenance Organizations (DSMOs). The DSMOs are:

1. Accredited Standards Committee X12
2. The Dental Content Committee
3. Health Level Seven
4. National Council for Prescription Drug Programs
5. National Uniform Billing Committee
6. National Uniform Claim Committee

These organizations will work together to accept and evaluate requests for changes to the standards and suggest changes to the standards for the Secretary's consideration. Further information about the change request process can be found on the Internet at: http://www.hipaa-dsmo.org/.

The Secretary may modify a standard or its implementation guide specification one year after the standard or implementation specification has been adopted, but not more frequently than once every 12 months. If the Secretary modifies a standard or implementation specification, the implementation date of the modified standard or implementation specification may be no earlier than 180 days following the adoption of the modification. The Department of Health and Human Services (HHS) will determine the actual date, taking into account the time needed to comply given the nature and extent of

the modification. HHS may extend the time for compliance for small health plans. Standards modifications will be published as regulations in the Federal Register.

17. Does the law require physicians to buy computers?

No, there is no such requirement. However, more physicians may **want** to use computers for submitting and receiving transactions (such as health care claims and remittances/payments) electronically, once the standard way of doing things goes into effect.

The Administrative Simplification provisions of the HIPAA law were passed with the support of the health care industry. The industry believed standards would lower the cost and administrative burdens of health care, but they needed Government's help to get to one uniform way of doing things. In the past, individual providers (physicians and others) have had to submit transactions in whatever form each health plan required. Health plans could not agree on a standard without giving their competitors a market advantage, at least in the short-run. The law, which requires standards to be followed for electronic transmission of health care transactions, levels the playing field. It does not require providers to submit transactions electronically. It does require that all transactions submitted electronically comply with the standards.

Providers, even those without computers, may want to adopt these standard electronic transactions, so they can benefit directly from the reductions in cost and burden. This is possible because the law allows providers (and health plans too, for that matter) to contract with clearinghouses to conduct the standard electronic transactions for them.

18. How will the standards affect data stored in my system?

The transaction standards will apply only to electronic data interchange (EDI) -- when data are transmitted electronically between health care providers and health plans as part of a standard transaction. Data may be stored in any format as long as it can be translated into the standard transaction when required. Security standards, on the other hand, will apply to all health care information.

To comply with the transaction standards, health care providers and health plans may exchange the standard transactions directly, or they may contract with a clearinghouse to perform this function. Clearinghouses may receive non-standard transactions from a provider, but they must convert these into standard transactions for submission to the health plan. Similarly, if a health plan contracts with a clearinghouse, the health plan may submit nonstandard transactions to the clearinghouse, but the clearinghouse must convert these into standard transactions for submission to the provider.

19. Can health plans require changes or additions to the standard claim?

Currently, some insurers accept the de facto standard claim (e.g., UB-92) but also require additional records (e.g., a proprietary cover sheet) for each claim submitted. Others have special requirements for data entered into the claim, which make it nonstandard.

Under the law, health plans are required to accept the standard claim submitted electronically. They may **not** require providers to make changes or additions to the standard claim. They must go through the private sector standards setting process to get their requirements added to the standard in order to effect desired changes. Health plans may not refuse the standard transaction or delay payment of a proper standard transaction.

An additional standard will be adopted for electronic health claims attachments, which health plans will be required also to accept. Until that standard is adopted (by February, 2001), health plans may

continue to require health claim attachments to be submitted on paper. No other additions to standard claims will be acceptable.

20. Should health plans publish companion documents that augment the information in the standard implementation guides for electronic transactions?

Additional information may be provided within certain limits.

Electronic transactions must go through two levels of scrutiny:

1. *Compliance with the HIPAA standard*. The requirements for compliance must be completely described in the HIPAA implementation guides and may not be modified by the health plans or by the health care providers using the particular transaction.
2. *Specific processing or adjudication by the particular system reading or writing the standard transaction*. Specific processing systems will vary from health plan to health plan, and additional information regarding the processing or adjudication policies of a particular health plan may be helpful to providers.

Such additional information may not be used to modify the standard and may not include:

- Instructions to modify the definition, condition, or use of a data element or segment in the HIPAA standard implementation guide.
- Requests for data elements or segments that are not stipulated in the HIPAA standard implementation guide.
- Requests for codes or data values that are not valid based on the HIPAA standard implementation guide. Such codes or values could be invalid because they are marked not used in the implementation guide or because they are simply not mentioned in the guide.
- Change the meaning or intent of a HIPAA standard implementation guide.

21. Could companion documents from health plans define cases where the health plan wants particular pieces of data used or not used?

The health plan must read and write HIPAA standard transactions exactly as they are described in the standard implementation guides. The only exception would be if the guide explicitly gives discretion regarding a data element to a health plan. For claims and most other transactions, the receiver must accept and process any transaction that meets the national standard. This is necessary because multiple health plans may be scheduled to receive a given transaction (e.g., a single claim may be processed by multiple health plans).

For example: Medicare currently instructs providers to bill for certain services only under certain circumstances. Once HIPAA standard transactions are implemented, Medicare will have to forego that policy and process all claims that meet HIPAA specifications. This does not mean that Medicare, or any other health plan, has to change payment policy. Today, Medicare would refuse to accept and process a bill for a face lift for cosmetic purposes only. Once the HIPAA standards are implemented, Medicare will be required to accept and process the bill, but still will not pay for a face lift that is purely for cosmetic purposes.

22. May health plans stipulate the codes or data values they are willing to accept and process in order to simplify implementation?

The simplest implementation is the one that is identical to all others. If the standard adopted stipulates that HCPCS codes will be used to describe procedures, then the health plan must abide by the instructions for the use of HCPCS codes. A health plan could refuse a code that was not applied in

accordance with the HIPAA national standard coding instructions, but could not refuse a code properly applied for reasons of policy unrelated to the standard.

For example, if the standard stipulates that the most specific code available must be used, then a health plan would be right to refuse a code that does not meet that criterion. The health plan would need to work with the committee(s) governing the particular coding scheme to have codes adopted that meet its needs.

23. May health plans stipulate the number of loop iterations or the file sizes they are willing to accept?

Any loop iterations, file sizes, etc. stipulated in the standards must be honored by all players. If any health care electronic data interchange participant cannot live with the numbers stipulated in the HIPAA implementation guides, then the participant needs to work with the implementation guide author(s) to get numbers that all players can live with.

For example, there are up to 99 service lines in a professional claim. The provider need not write 99 service lines, but the health plan must have the capability to accept that number when presented. If that is not the right number for all players, it should be changed. But the number identified in the implementation guide must be adhered to.

PRIVACY STANDARDS

1. **What about faxed transmissions?**

   Fax imaging and voice response transmissions are not subject to the HIPAA transactions standards but may have to meet privacy and security standards. Health plans may continue to offer these services, however, they must still be able to accept and send the HIPAA standard transactions.

2. **On a call back to the patient to remind them of their appointment, if there is no answer, can we leave a message on their answering machine as to when their next appointment is?**

   Answering machines are tricky! What if the doctor is an obstetrician and a message is left to say that the next appt is.....? Is that letting the cat out of the bag so to speak?

   I would think that common sense needs to be applied here. I don't think that the doctor's name or practice name should be left. Perhaps something like "Ms Gamp, this is your doctor's office calling to remind you of your next appointment." That's pretty innocent.

3. **Is there a federal privacy protection today?**

   Today, privacy protection is provided by the States.

4. **Is this privacy protection consistent across the States?**

   State laws and their protections are uneven and leave large areas uncovered.

5. **How much of my personal information is going to be released?**

   The new standards put in place how such information should be released. Privacy protections must be balanced with the public responsibility to support such national priorities as protecting public health, conducting medical research, improving the quality of care, and fighting health care fraud and abuse. For example, public health agencies routinely use health records in their efforts to protect the public from outbreaks of infectious diseases.

6. **What does the Privacy Standard provide?**

   This standard defines the use and disclosure of health information. It establishes individual patient rights and the health information that is covered. It also requires that providers, plans, and clearinghouses adopt policies for safeguarding this information.

7. **Who can use my health information?**

   With your individual consent, your health information can be used for treatment, payment or health care operations. It can be used for public health reasons or enforcement of compliance review by DHHS.

8. **Can my information be used for other uses such as hospital fund raising or marketing?**

   For other uses, an individual authorization would be needed.

9. Is there any assurance that my information has not been released if I do not sign an individual authorization?

This standard also provides that the provider, plan, or clearinghouse provide an audit trail of where your information was disclosed.

10. I want to review my recent hospitalization records. Can I do that?

Under this standard you have the right to review them. Currently, many states do not encourage patients to review their records and actually discourage them.

SECURITY AND ELECTRONIC SIGNATURES

1. Why are there standards for Security and Electronic Signature?

The standard has been created to ensure confidentiality and integrity of health information of individuals.

2. Why is there a need for standards for Security and Electronic Signature?

Currently, there is no consistent protection of individual health information. HIPAA's regulations will protect the individual's health information. At the same time the standard allows this information to be accessible to appropriate healthcare providers, clearing houses, and health plans. A new electronic signature standard has also been developed for consistency if required by future HIPAA standard transactions for any transaction that involves a HIPAA standard transaction.

3. What are the main requirements of the Security Standards?

There are four areas of requirements:

1. **Information systems security**, requiring the protection of all affected computers and data from compromise or loss;
2. **Physical security**, requiring protection of all buildings, facilities and assets from compromise or threat;
3. **Audit trail**, requiring keeping audit trails of access to patient identifiable information; and
4. **Digital signature/data encryption**, requiring transmissions to be authenticated and protected from observation or change.

4. How will the Security Standards solve problems?

A minimum standard of protection will be established wherever individual health information is stored electronically or transported over telecommunication systems. This minimum does not exist today.

5. How will the Electronic Signature Standard solve problems?

This standard provides a method for ensuring the integrity of the message, authentication of the user, and non-repudiation.

6. Who must comply with the Security Standards?

Any healthcare provider, health care clearinghouse, health care plan or other healthcare entity must comply if they maintain or transmit health information of an individual electronically.

7. Who must comply with the Electronic Signature Standard?

If an electronic signature is used in transactions covered by HIPAA or in the future required by HIPAA, then any health care provider, clearinghouse, plan or other healthcare entity must comply.

8. We are not currently using an electronic signature. Do I have to initiate this project?

HIPAA does not require an electronic signature at this time.

9. Do the Security Standards apply just to transactions covered by HIPAA as the Electronic Signature Standards do?

The standards are applicable to all individual health information that is in an electronic form.

10. What about hard copies of individual health information?

The security standards only apply to electronic forms at this point.

11. Does the Security Standard specify a technology to be used?

HIPAA has been designated as "technology neutral." This allows each business to select the right technology that will meet the basic requirements for the individual environment.

12. How do the standards affect all the data that is stored in my system?

The standards have no affect on how your data is stored. Your data must be able to be translated into the standard transaction when required for electronic data interchange (EDI) between health care providers and health plans as part of a standard transaction.

UNIQUE IDENTIFIERS

1. Why is a Standard for an Employer Identifier Number (EIN) needed?

There are many instances where employers need to be identified. Since many employers sponsor health insurance for their employees, using a single identifier for the employer would simplify electronic transactions. Employers may need to be identified by healthcare providers when claims for their employees' care are submitted electronically. In another instance, employers need to be identified when enrolling or disenrolling employees in health plans or when making premium payments.

2. What number is being proposed for the EIN?

The taxpayer identifying number that the Internal Revenue Service assigns has been proposed as the EIN.

3. Do all employers have this taxpayer identifying number?

It is a requirement that any employer who pays wages to one or more employees must have the taxpayer identifying number.

4. Don't some employers have more than one taxpayer identifying number?

Yes.

5. Which taxpayer identifying number (EIN) are they to use if they have more than one?

Public comment regarding which of the taxpayer identifying numbers should be used has been requested by DHHS in the Notice of Proposed Rule Making (NPRM). This issue has not yet been resolved.

6. Who is responsible for using the EIN?

Employers do not have to use the EIN in standard transactions at this time under HIPAA, but may choose to use it. Employers are required to share their EIN for purposes of using the number in standard transactions. Health Plans, Clearing Houses, and Providers must use the EIN in electronic transactions if the EIN is required in a document.

7. What is the National Provider Identifier (NPI)?

Currently, each health plan assigns numbers to health care providers-individuals, groups, or organizations that supply health care. If the provider does business with multiple plans, he/she will have multiple numbers. The proposed NPI will be unique for the provider. Each health plan will use the same NPI for that provider. What specifications have been proposed for the NPI? In the Notice of Proposed Rulemaking (NPRM), the NPI is designed to be 8 digits. The final digit has no embedded intelligence. It is used to detect keying errors and is a check digit.

8. Who would be given an NPI?

According to the NPRM, any health care providers who need to submit claims or transactions as outlined in HIPAA would need an NPI.2. The Notice of Proposed Rulemaking proposed that NPIs

would be given to health care providers that need them to submit claims or conduct other transactions specified by HIPAA.

9. Who are considered health care providers?

A health care provider is an individual, group, or organization that provides medical or other health services or supplies. This includes physicians and other practitioners, physician/practitioner groups, institutions such as hospitals, laboratories, and nursing homes, organizations such as health maintenance organizations, and suppliers such as pharmacies and medical supply companies.

10. Who are not considered health care providers?

Individuals who work in these industries but who do not provide health care services would not be issued an NPI. Examples of this would be admission clerks, billing personnel, aides and orderlies. These individuals support healthcare but do not provide care.

11. How will NPIs be issued?

The National Provider System (NPS) would issue NPIs based upon information entered into the NPs "Enumerators" would be responsible for entering identifying information about the health care providers, validating data such as State license number, notifying the health care provider of the NPI. The "enumerators" would also be responsible for updating the health care providers' information.

12. Who or what are "enumerators?"

This was another area where the Notice of Proposed Rulemaking sought comments on the proposals that were listed. HCFA files have the data needed to enumerate Medicare providers so that data would be loaded into the NPs first and an NPI would be assigned to each Medicare provider. These providers would not have to apply for an NPI under either option. There are two options that are being considered for other health care providers to get an NPI:

Option 1: The enumerator of all health care providers would be a Federally-directed registry

Option 2: A registry would be enumerators for a combination of Federal programs (health plans) and Medicaid State agencies.

13. How would Option 1 work?

Option 1: All other health care providers would apply for an NPI to a registry that could be operated by an agent or contractor. The registry would enter the provider's data into NPs NPs would assign an NPI and the registry would notify the provider.

14. How would Option 2 work?

Option 2: Federal programs and Medicaid State Agencies would enumerate their own health care providers by entering the data into the NPs The NPs would assign NPIs to the providers. If a provider participated in more than one Federal or Medicaid health plan, a choice could be made as to which it wishes to be enumerated.

15. How will NPIs be used?

NPIs must be used in connection with the electronic transactions that HIPAA has identified. NPIs can also be used to identify other health care providers in health care transactions or correspondence. Health plans can also use NPIs to communicate with health care providers. Clearinghouses can use NPIs when communicating with health care providers and plans. NPIs could also be used by DHHS to cross reference health care providers in fraud and abuse files.

16. Currently, Unique Physician Identifier Number (UPIN) exists in the Medicare program for identification. Will there be any relationship between UPIN and NPI?

NPI will eventually replace the UPIN. For transactions specified by HIPAA, NPI and UPIN will not be used concurrently.

17. Will foreign health care providers be assigned an NPI?

The NPs will assign NPIs to foreign health care providers who conduct electronic transactions, such as claims, with US health plans that are covered by HIPAA.

18. Is there a difference between the PlanID and the NPI or are they the same?

They are different. The PlanID will be assigned to health plans. NPIs will be assigned to health care providers. On some occasions, an organization will receive a PlanID and an NPI. One instance where this could occur is when a managed care organization is both a health plan and a health care provider.

19. What is the difference between the health plan identifier (PAYERID) and PlanID?

PlanID was formerly known as PAYERID.

20. What is a Unique Identifier for Individuals?

It is exactly what the term indicates. Each individual would be identified with one identifier that would be unique to that person.

21. What is happening with the Individual Identifier? Will we have one or not?

Currently the funding for development of a national individual identifier is on hold. According to DHHS, opinion about the unique identifier for individuals is deeply divided. The Clinton-Gore Administration deemed it wise to wait on the establishment of an individual identifier until after the other HIPAA security and privacy provisions were in place. Since the intent of the individual identifier is to positively identify the individual's health information across the care continuum, adequate security and privacy measures will need to be in place first to ensure no loss in privacy or security occurs with the use of the individual identifier.

22. Why would an Individual Identifier be needed?

HIPAA recognized the need for a unique individual identifier as part of the administrative simplification process. Today, the various health care providers assign individuals numbers for purposes of their own identification process and obviously these numbers are not cross-referenced. A unique individual identifier will allow for the reduction of administration workload and costs, enable faster access to critical health information, and increase the efficiency in the exchange of electronic data.

Duplicate medical record numbers and disparate medical files have plagued the health care industry, due to many reasons. Individuals may not present themselves accurately or in the same manner for

each individual episode of care, such as the use of nicknames, name changes due to marriage or divorce, or misspelling of one's name. Health care staff may not select or retrieve the appropriate record due to the previous reasons, misfilings, or inadvertent error. Studies have documented intentional misrepresentation by the patient as a mechanism to protect their privacy.

A secure and privacy-protected individual identifier would allow for positive identification, collection and retrieval of the medical record and ensure that health care professionals have access to the complete set of patient information. Quality health care depends upon the ability to aggregate the patient's information to synthesize an accurate complete profile of the patient's health status.

23. Everyone has a Social Security Number, why not use that as the unique identifier?

There is concern by many individuals and groups that if the Social Security Number is used there will be extended linking not only for health information but also credit and financial information. That is definitely not the intent of the individual unique identifier.

ADMINISTRATIVE SIMPLIFICATION COMPLIANCE ACT (ASCA)

1. What is the HIPAA Administrative Simplification Compliance Act (ASCA)?

In December 2001, the Administrative Simplification Compliance Act (ASCA) extended the deadline for compliance with the HIPAA Electronic Health Care Transactions and Code Sets standards (codified at 45 C.F.R. Parts 160, 162) one year to October 16, 2003 for all covered entities other than small health plans (whose compliance date was already October 16, 2003).

In order to receive an extension, covered entities must submit their ASCA compliance plans on or before *October 15, 2002*.

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.

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 is 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.

2. Where can I get a copy of the ASCA compliance form?

The form was released on March 28, 2002 and is available on CMS' website at **http://www.cms.hhs.gov/hipaa/hipaa2/ASCAForm.asp**. The form was published in the Federal Register on April 15, 2002.

3. Is my organization supposed to submit our entire detailed compliance plan?

No. The compliance extension form asks only for summary information from your detailed plan. You do not need to send other information.

4. Does the law require Medicare claims to be submitted electronically after Oct. 2003?

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.

5. What will be the impact of the one-year ASCA extension?

The delay will give covered entities more time to build, test, and successfully implement the Final Electronic Health Care Transactions and Code Sets required by HIPAA.

6. How extensive will the model compliance extension form be?

The form is simple and easy to complete. 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;
4. a timeframe for testing to begin no later than April 16, 2003.

7. Do software vendors need to file for an ASCA extension?

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.

8. Is HHS going to actually review & approve all ASCA compliance plans?

Submission of a properly completed compliance extension plan is sufficient to secure the one-year extension.

9. Can I file the ASCA compliance extension form electronically?

Yes, we encourage electronic filing of compliance extension plans, although we will also accept plans submitted on paper. To submit a form electronically, go to http://www.cms.hhs.gov/hipaa/hipaa2/ASCAForm.asp.

10. Does the ASCA extension affect the compliance date for the HIPAA privacy standards?

No, the compliance date for the privacy standards is still April 14, 2003 or, for small health plans, April 14, 2004.

11. Do all covered entities automatically get an ASCA extension?

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.

12. Why didn't Congress just give everyone an ASCA extension?

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.

13. Will noncompliant covered entities that fail to file an ASCA compliance plan be excluded from Medicare?

HHS will be publishing proposed regulations to address this new exclusion authority.

14. Will some ASCA compliance plans be denied?

Submission of a properly completed compliance plan is sufficient to secure the one-year extension.

15. Do I have to use the ASCA form?

The compliance extension form we developed is a model. While we strongly recommend its use, covered entities may submit plans using other formats.

16. How does the ASCA delay affect Medicare implementation activities?

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.

17. When will Medicaid Agencies test ASCA compliant transactions with trading partners?

Each Medicaid State Agency has its own project plan for achieving HIPAA compliance, and will decide whether to submit a compliance 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.

18. Should covered entities discontinue testing until 2003?

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.

19. Can small health plans get an ASCA extension to their current compliance date?

No, the compliance date for small plans does not change; it remains October 16, 2003.

20. Where should I send my completed ASCA compliance form?

Please submit your ASCA compliance form electronically via our website. If you cannot submit your compliance plan electronically, it must be printed and mailed to us. Send to:

Model Compliance Plans
Centers for Medicare and Medicaid Services
P.O. Box 8040
Baltimore, MD 21244-8040

21. Must I file an ASCA compliance plan to communicate with noncompliant partners?

No. A covered entity is not required to conduct compliant transactions with covered entities that are not yet required to be in compliance and therefore would not need to submit an ASCA compliance extension plan.

22. How will an entity know if another entity has filed an ASCA compliance plan?

Should an entity need to determine if another entity has filed a compliance plan, that entity should communicate directly with the other entity (i.e., 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.

23. How does the delay affect Medicare implementation activities?

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.

24. Can plans make network providers move to standard transactions before 10/16/03?

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.