



HIPAA

Health Insurance Portability
and Accountability Act

How to “HIPAA” – Top 10 Tips

.....

1. Understand the deadlines and move to compliance.
2. Know your compliance requirements.
3. Prioritize your compliance activities.
4. Ask the right questions.
5. Choose and use consultants wisely.
6. Learn from trusted sources.
7. Separate fact from fiction.
8. Visit Web site resources often for the latest updates.
9. Talk to your patients.
10. Look to the AMA for updates.

www.ama-assn.org/go/hipaa

These materials do not constitute legal advice and are for educational purposes only. The information in this packet is based on current federal law and subject to change based on changes in federal law, the effect of state law or subsequent interpretative guidance.

How to “HIPAA”— Tip #1

Understand the deadlines and move to compliance.

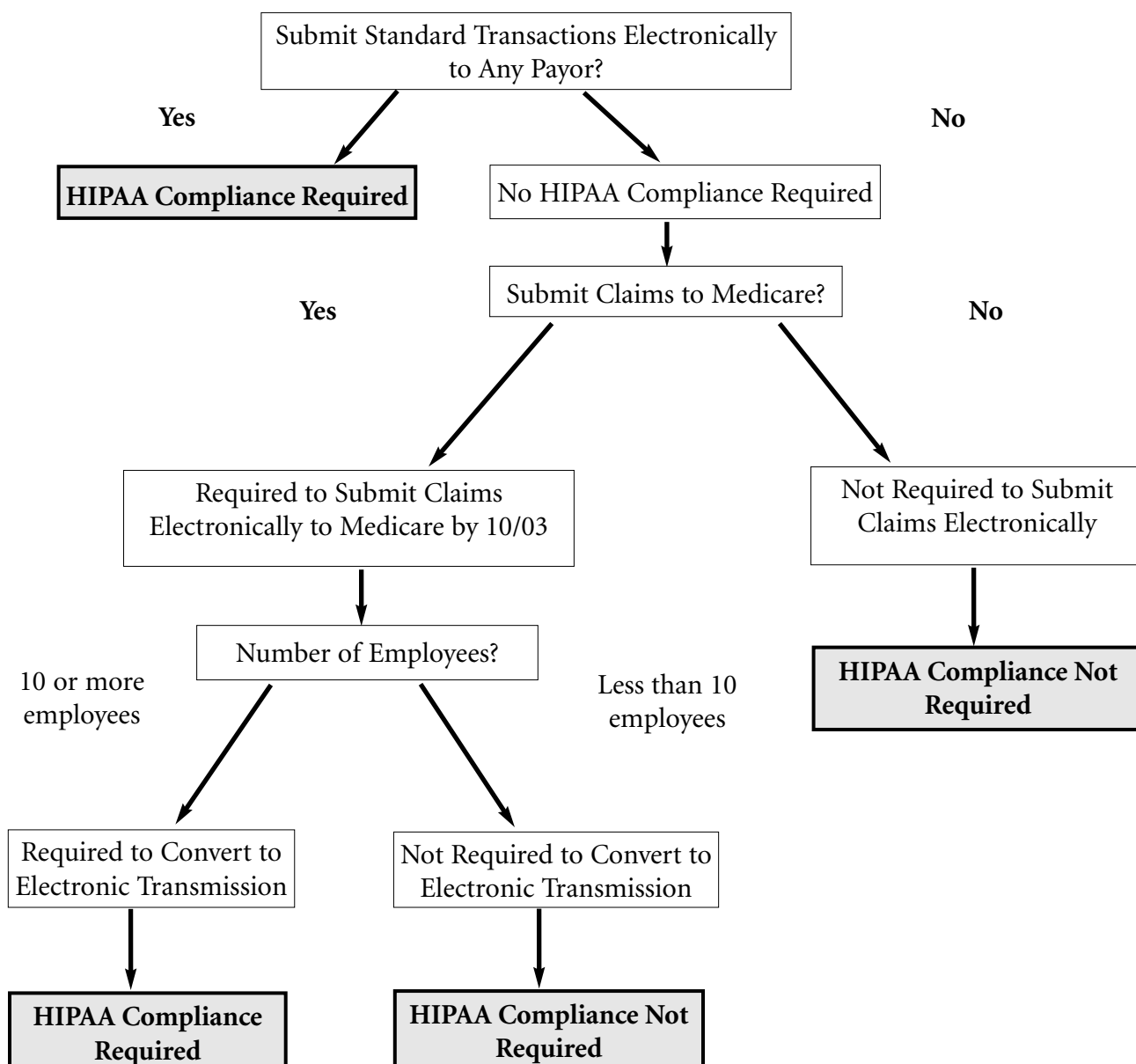
Standard	Description	Compliance Date	Implications
Transaction and Code Set Standards	Standardizes the format for electronic transactions between physicians and health plans. Standard HIPAA code sets include large code sets like CPT.	10/16/03	Fines are not to exceed \$100 per violation per person or entity. The total amount imposed on any one person, for violation of any one requirement, may not exceed \$25,000 in each calendar year.
Medicare Requirement to Submit Electronic Claims	Physicians must submit their claims to the Medicare program in the standard electronic format. Physician practices with fewer than 10 full-time employees are not subject to this standard.	10/16/03	Medicare contractors will not accept transactions that do not meet the new standards, i.e., electronic format, after compliance date.
Privacy	Regulates how protected health information may be used and disclosed; it also provides certain rights to patients and contains administrative requirements to protect confidentiality of protected health information.	4/14/03	Fines are not to exceed \$100 per violation per person or entity. The total amount imposed on any one person, for violation of any one requirement, may not exceed \$25,000 in each calendar year. Criminal fines and penalties may be imposed if protected health information is used or disclosed with the requisite intent.
Privacy – Business Associates	<p>Business associates perform certain functions, activities or services on behalf of the physician involving the use and/or disclosure of protected health information.</p> <p>New agreements and existing agreements with a renewal date prior to April 14, 2003 must be either amended, or terminated and replaced with new agreements containing HIPAA's required provisions as the earlier renewal date or by April 14, 2003.</p> <p>Existing agreements with renewal by its terms after April 14, 2003 (including contracts with an automatic renewal date) must be either amended, or terminated and replaced with new agreements containing HIPAA's required provisions by April 14, 2004.</p>	4/14/04	<p>Physicians are not required to actively monitor the means by which the business associate carries out the safeguards of the contract.</p> <p>Physicians are not liable for privacy violations of a business associate, unless the physician becomes aware of a practice of the business associate that constitutes a violation of the business associate's obligations under its contract. In that case, the physician must take “reasonable steps” to end the violation. If such steps are not successful, the physician must terminate the contract, if feasible, or report to the Secretary of the HHS.</p> <p>A physician would be considered out of compliance with the requirements of the rule only if the physician fails to take the steps described above after becoming aware of the violation.</p>
National Employer Identifier	Standardizes the way employers are identified in electronic transactions: a unique ID number for each employer will be assigned based on the employer's Federal Employer Identification Number.	7/30/04	Fines are not to exceed \$100 per violation per person or entity. The total amount imposed on any one person, for violation of any one requirement, may not exceed \$25,000 in each calendar year.
Security Standards	Requires the establishment of procedures and mechanisms to protect the confidentiality, integrity and availability of electronic protected health information. Physicians must implement administrative, physical, and technical safeguards for protected health information that they collect, maintain, use or transmit.	4/21/05	Fines are not to exceed \$100 per violation per person or entity. The total amount imposed on any one person, for violation of any one requirement, may not exceed \$25,000 in each calendar year.

How to “HIPAA”— Tip #2

Know your compliance requirements.

HIPAA: Who Must Comply?

The following series of easy “yes” and “no” questions is designed to be a simple test to help physicians determine whether or not they must comply with the privacy, security, transactions and other related standards of HIPAA. If the test determines compliance is necessary, the AMA has a variety of educational offerings that can be reviewed by visiting <http://www.ama-assn.org/ama/pub/category/4234.html>



How to “HIPAA”— Tip #3

Prioritize your compliance requirements.

Understanding targets for compliance

- Federal
- State
- Regulatory changes and guidance

Evaluate current office practices by conducting a gaps analysis/risk assessment

- Complete operational assessment
- Evaluate paper systems and forms
- Assess information systems
- Conduct contract evaluation
- Review policies and procedures
- Determine existing responsibility for the privacy function
- Perform due diligence on your business relationships

Educate employees

Educate patients

Establish compliance systems and a plan

- Establish a plan and a budget
- Create documentation
- Develop training
- Monitor office practices and follow-up
- Identify responsible Privacy Contact
- Test information systems

Manage the Business Associate and other relationships

How to “HIPAA”— Tip #4

Ask the right questions.

To ensure that your claims for payment and other electronic transactions are HIPAA compliant by October 16, 2003, you should be asking the right questions of your software vendors, billing services and clearinghouses.

It is important to ask these questions to avoid delays in payment as these entities become HIPAA compliant.

Your software vendor should provide you with HIPAA compliant system upgrades that have been successfully tested with payors. Billing services and clearinghouses should also be able to demonstrate completion of successful testing with payors.

To assist you in your discussion, following is a series of questions to ask software vendors and billing companies/clearinghouses. Definitions of terms are also provided.

General Questions

1. Will systems upgrades require a new version of my software or additional hardware? If so, is this included as a free upgrade under my contract?
2. What is the name of your HIPAA Compliance Officer and how do we contact them?
3. Will your software or billing service/clearinghouse (as applicable) enable me to send to all payors a claim/encounter form (the old HCFA 1500 form or National Standard Format - NSF) in the HIPAA standard 837 content and data format?
4. Does your system gather all data elements (required and situational)?
5. When will you be sending me a schedule of testing that includes (1) internal testing, (2) testing with a clearinghouse, (3) testing with Medicare, and (4) testing with commercial payors? Are you currently on schedule for testing? What will it cost?
6. Will testing be certified by a third party?
7. What must my organization do to prepare to test?
8. On what date will you be ready to convert the new HIPAA-compliant format?
9. Are there other transactions that you will provide in addition to claims payment such as claims status and eligibility checks?
10. What, if anything, is my office responsible for completing prior to making this transition? By when? How do I get assistance with these activities?

11. How will you communicate to us what is wrong with a rejected transaction?
12. Does your organization have access to the payors' "companion guides"?
13. Does your system have backups for component failure?
14. Is security an up-front design consideration with your system?
15. What is your contingency plan to ensure that my cash flow is not disrupted with the payors?
16. Will your system allow direct transmission to payers or will the services of a clearinghouse be required?
17. If a clearinghouse is required, can it be one of my own choosing?

Questions for Clearinghouses

1. What information is available regarding your plan for compliance and the status?
2. What is the name of your HIPAA Compliance Officer and how do we contact them?
3. Will you be using a third-party to test and certify transaction compliance?
4. What must my organization do to prepare to test?
5. Do you have access to the payors' "companion guides" and when will you begin to edit transactions for compliance?
6. Have you identified a minimum data set for the transactions, especially the claims transaction?
7. What changes, if any, will be made to service fees?
8. What is the process for Business Associate Agreements?
9. What support services are available to me?
10. What is your contingency plan to ensure that my cash flow after October 16th, 2003 is not disrupted with the payors?

Other Useful Questions for Third Party Administrators ("TPA")/Payors/Carriers

1. Ask for their "companion guides." These guides will provide helpful information regarding submitting claims to the specific TPA/payor/carriers requirements for a complete transaction.
2. What is the name and title of your HIPAA Compliance Officer?
3. Ask them what new data fields they are adding to their systems, so that you will know what information to collect from your patients.

4. Will you be offering any new “HIPAA services” such as browser based applications for claims status inquiries, authorization/referral requests, eligibility, etc.?
5. What is your contingency plan to ensure that my cash flow after October 16th 2003 is not disrupted?

Definitions

Testing – the process of conducting transaction trials between entities to ensure that the electronic transactions function and are completed in accordance with HIPAA

Health Care Clearinghouse – means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:

- (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
- (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Transaction – means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

- (1) Health care claims or equivalent encounter information.
- (2) Health care payment and remittance advice.
- (3) Coordination of benefits.
- (4) Health care claim status.
- (5) Enrollment and disenrollment in a health plan.
- (6) Eligibility for a health plan.
- (7) Health plan premium payments.
- (8) Referral certification and authorization.
- (9) First report of injury.
- (10) Health claims attachments.
- (11) Other transactions that the Secretary may prescribe by regulation.

How to “HIPAA”— Tip #5

.....
Choose and use consultants wisely.



HIPAA Consultants and Attorneys are Just a Phone Call Away

Finding a HIPAA advisor is easy. But finding the right HIPAA advisor can be a challenge. That’s why the AMA ConsultingLink network, a national network of attorneys and consultants, now includes healthcare lawyers and consultants with HIPAA expertise.

Our network of professionals can assist you with all of your HIPAA needs, including:

- Review of business associate contracts
- Review of employee contracts
- Gap analysis
- Risk assessment
- Implementation of compliance plans
- Ongoing monitoring
- HIPAA litigation

Call 800-366-6968 today for a FREE referral to an expert in your area.

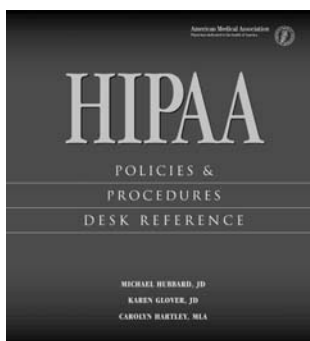
How to “HIPAA”— Tip #6

.....
Learn from trusted sources.

Take the next step *toward HIPAA compliance*

The HIPAA Privacy Rule requires that you develop policies and procedures for your office and provide privacy training to your staff. These resources from the American Medical Association can help you meet those requirements, putting you one step ahead in your HIPAA compliance plan.

Create HIPAA policies and procedures that you can implement with confidence



HIPAA Policies and Procedures Desk Reference,

written by authors of the AMA's *Field Guide to HIPAA Implementation*, addresses cultural and regulatory changes regarding patient privacy and offers a wide range of HIPAA policies and procedures that physicians and privacy officers can customize for their medical practices.

to the specific policy for each HIPAA question, a basic overview of HIPAA policies and procedures, and additional in-depth support and answers to more complex questions.

What follows are 39 comprehensive policies and procedures that address components of topics such as protected health information, patient rights, and privacy management. Because these policies and procedures – plus 57 sample forms – are included on the accompanying CD, medical practices can customize them easily to fit individual needs.

Available February 2003

Three-ring bound, 496 pages

Order #: OP319602 ISBN: 1-57947-362-8

Price: \$199.95

AMA Member Price: \$159.95

The first section offers an overview of the Privacy Rule with guidelines physicians should follow, a quick reference guide that points

Meet HIPAA privacy training requirements with this unique multimedia tool

The ***HIPAA Privacy Tool Kit***

guides your office through the basics of the Privacy Rule and teaches the important role the medical practice staff plays in protecting patients' rights.

The kit includes material for two training levels plus:

- A 22-minute training video (also available in DVD format) that provides a general overview of the HIPAA Privacy Rule and more than two dozen examples of oversights and ways to protect your practice from privacy violations
- An audio CD of interviews with nationally recognized leaders offering real-world perspectives on the Privacy Rule
- A 16-page *HIPAA Privacy 101 Handbook*, which breaks the rule into easy-to-digest nuggets with questions at the end to test and ensure understanding



■ A *HIPAA Privacy Pocket Guide* that provides expanded information about the Privacy Rule in a concise, informative, 44-page format

■ Sample documents, including a Notice of Privacy Practices and a business associate agreement

■ Wall charts and posters that introduce employees to the new rules and vocabulary
Tool kit users also will be able to download current privacy information and discussion questions from a dedicated Web site.

Order #: OP320002

ISBN: 1-932246-00-2

Price: \$599.00

AMA Member Price: \$525.00

To receive the kit with the training video on DVD, use order # OP320202.

How to “HIPAA”— Tip #7

Separate fact from fiction.

Department of Health and Human Services, Office for Civil Rights True Or False Quiz

- Patient:** My doctor needs to discuss my treatment with other doctors and nurses. But the Privacy Rule prohibits doctors and nurses from discussing private health information if there is a possibility that someone will overhear. What if my doctor needs to discuss my condition with a nurse at a busy nursing station, or with me over the phone from someplace other than a private office? The privacy rule prevents these discussions.
- False!** *The Privacy Rule is not intended to prohibit providers from talking to each other and to their patients.*
- Patient:** The privacy rule will create a government database with all individual’s personal health information.
- False!** *The rule does not require a physician or any other covered entity to send medical information to the government for a government database or similar operation.*
- Patient:** The privacy rule prevents a friend or family member from picking up prescriptions for me. Now I’ll have to get out of my sick bed to get my medicine.
- False!** *The Rule allows a pharmacist to use professional judgment and experience with common practice to make reason-able inferences of the patient’s best interest in allowing a person, other than the patient, to pick up a prescription.*
- Physician:** The privacy rule requires me to monitor the activities of my business associates.
- False!** *Covered entities are not required to monitor or oversee the means by which the business associate carries out safeguards or the extent to which the business associate abides by the requirements of the contract.*
- Physician:** The privacy rule prevents me from using a sign-in sheet so I can know when a patient has arrived. I can’t even call out the names of patients in the waiting room when its their turn for their appointment.
- False!** *The Department did not intend to prohibit the use of sign-in sheets or the practice of calling patients’ names in the waiting room when it is time for their appointments and clarified this in the July 6 guidance.*
- Hospital:** The privacy rule prohibits semi-private rooms. With two patients in a room, there is no way to guarantee that one won’t overhear health information about the other. Now I’ll have to rebuild my facility to include only private rooms.
- False!** *The Privacy Rule does not require these types of structural changes be made to facilities. Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.*

Hospital: The privacy rule allows doctors and nurses to see a patient's entire medical record, if they think they need it to do their jobs.

True! *The Privacy Rule does not prohibit use or disclosure of, or requests for an entire medical record. The covered entity must document in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes.*

Physician: The privacy rule requires covered entities to purchase expensive computer equipment.
False! *The Privacy Rule requirements do not require any particular technologies or types of technologies. They are flexible and scalable to the covered entity's information needs and information systems.*

Insurer: How are we supposed to do business under this Rule? It would prohibit doctors from faxing information to us, or to each other, or to their patients.

False! *The Rule does not prohibit faxing of individually identifiable health information. Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.*

Insurer: What happens when I am required to report information under state law? I assume that if some other law requires me to disclose health information, I won't have to do a big analysis under the privacy rule, or get caught in the middle because the privacy rule might not allow the disclosure?

True! *A disclosure of identifiable health information that is required by another law is permitted by the Privacy Rule.*

Anyone: The Privacy Rule is delayed by the Administrative Simplification Compliance Act that was passed in December 2001.

False! *This law delays compliance with the Transaction and Code Set standards for covered entities that file a compliance plan. This law does not apply to the Privacy Rule. The compliance date for the Privacy Rule is still April 14, 2003. (April 14, 2004 for small health plans).*

Patient: The Privacy Rule requires my doctor to give my health information to researchers and the police (even if they don't have a warrant) and health plans, all they have to do is ask.

False! *The Rule permits such disclosures under specified circumstances, but does not require them. In some cases, like research, an individual's authorization may be required. However, even when an authorization is not required and a disclosure is permitted by the Rule, there may be limitations or other requirements on such disclosures.*

Patient: When my family member comes to pick me up from the hospital, the doctor will still be able to explain my condition and tell him what to expect when I return home. Right?

True! *The Rule permits doctors to discuss a patient's condition with family or friends involved in the person's care, unless the patient objects.*

Family Member: The Privacy Rule would have prevented me from finding out information about my son in a hospital in New York on September 11.

False! *The Rule permits hospitals and disaster relief agencies to notify family members that a loved one has been admitted to a hospital or has been involved in a disaster.*

How to “HIPAA”— Tip #8

.....
Visit Web site resources often for the latest updates.

American Medical Association HIPAA Link (AMA)

<http://www.ama-assn.org/ama/pub/category/8910.html>

AMA HIPAA Link is an internet-based HIPAA education and compliance service. By subscribing to AMA HIPAA Link, physician practices will have access to all of the materials, guidance and record keeping required for a small healthcare organization to become and remain compliant with the HIPAA privacy and security regulations.

Centers for Medicare and Medicaid Services (CMS)

<http://www.cms.gov/hipaa/hipaa2/default.asp>

This link to the CMS web site includes general information (such as HIPAA background, frequently asked questions, compliance deadlines, and decision tools). This site also contains information about the enforcement process, educational materials, latest news, upcoming events and HIPAA related links.

US Department of Health and Human Services (DHHS)

<http://aspe.os.dhhs.gov/admsimp>

This Department of Health and Human Services web site includes information dealing with the administrative simplification provisions of HIPAA of 1996. This site contains general information about the administrative simplification portion of the HIPAA law, an explanation of the Notice of Proposed Rulemaking (NPRM) process, update on when HIPAA standards may be implemented, and educational information.

National Uniform Claim Committee (NUCC)

www.nucc.org

This links to the Web site for the NUCC, that is chaired by the American Medical Association. The NUCC was formally named in the administrative simplification section of the HIPAA of 1996 as one of the organizations to be consulted by the American National Standards Institute’s accredited Standard Designating Organizations and the Secretary of HHS as they develop, adopt, or modify national standards for health care transactions. As such, the NUCC is intended to have an authoritative voice regarding national standard content and data definitions for non-institutional health care claims in the United States.

Workgroup for Electronic Data Interchange (WEDI)

<http://www.wedi.org/>

This is the Workgroup for Electronic Data Interchange web site. This site includes among other things, information on EDI in the health care industry, lists of conferences, implementation information and the availability of resources for standard transactions.

Phoenix Health Systems HIPAA Advisory

<http://www.hipaadvisory.com>

This web site provides a wide breadth of topics on news, compliance tips and other valuable information. Various HIPAA resources are also available on this web site.

National Committee on Vital and Health Statistics (NCVHS)

<http://www.ncvhs.hhs.gov>

This is the National Committee on Vital and Health Statistics web site. NCVHS is the Advisory Body to the Department of Health and Human Services. Information on membership, how to contact the committee, announcements and agendas for past and future public hearings is also available.

Medicaid

<http://www.hcfa.gov/medicaid/hipaa/adminsim/default.htm>

This site contains Medicaid HIPAA Information - including Medicaid HIPAA Plus, the Medicaid HIPAA-Compliant/Concept Model, Informational briefs, Implementation tools, and National Medicaid EDI HIPAA Workgroup Information.

Medicare

<http://www.hcfa.gov/medicare/edi/edi.htm>

This is the Medicare EDI web page. At this site you will find information regarding Medicare EDI, advantages to using Medicare EDI, Medicare EDI formats and instructions, news and events, frequently asked questions about Medicare EDI, and information regarding Medicare paper forms and instructions.

How to “HIPAA”— Tip #9

Talk to your patients.

Dear Physician:

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) establishes federal standard formats and data content for electronic transactions between physicians and health plans. HIPAA also outlines how the health information of patients may be used and disclosed, identifies patients’ privacy rights and requires certain privacy practices of physicians, health plans and other health care providers. In addition, HIPAA requires the development and implementation of administrative, technical and physical safeguards to ensure the security of patients’ health information.

If you transmit claims in an electronic format, you will be required to provide adequate notice of privacy practices to your patients at your office when providing them services for the first time. The “Notice of Privacy Practices,” will provide your patients with an overview of your office’s privacy practices as well as an understanding of the patient’s privacy rights and the limits of those rights. You will also be required in most situations to make a good faith effort to obtain a written acknowledgement from the patient that they received the Notice of Privacy Practices.

Attached is a sample letter that you may wish to provide to your patients to give them a general understanding of the scope and purpose of HIPAA and to introduce your Notice of Privacy Practices. Please use this sample letter to suit your own practice. This sample letter is not required by law, but it may serve as a useful tool to assist your patients in understanding the purpose of the privacy rule.

Dear Patient:

Physicians have always protected the confidentiality of health information by locking medical records away in file cabinets and refusing to reveal your health information. Today, state and federal laws also attempt to ensure the confidentiality of this sensitive information.

The federal government recently published regulations designed to protect the privacy of your health information. This “privacy rule” protects health information that is maintained by physicians, hospitals, other health care providers and health plans. As of April 14, 2003, your physician will need to comply with the privacy rule’s standards for protecting the confidentiality of your health information.

This new regulation protects virtually all patients regardless of where they live or where they receive their health care. Every time you see a physician, are admitted to the hospital, fill a prescription, or send a claim to a health plan, your physician, the hospital and health plan will need to consider the privacy rule. All health information including paper records, oral communications, and electronic formats (such as e-mail) are protected by the privacy rule.

The privacy rule also provides you certain rights, such as the right to have access to your medical records. However, there are exceptions; these rights are not absolute. In addition we will be taking even more precautions in our office to safeguard your health information such as training our employees and employing computer security measures. Please feel free to ask your physician or our privacy contact about exercising your rights or how your health information is protected in our office.

The Notice of Private Practices attached to this letter explains our privacy practices. It contains very important information about how your protected health information is handled by our office. It also describes how you can exercise your rights with regard to your protected health information.

Please let us know if you have any questions about our Notice of Privacy Practices. You may contact our privacy contact at _____, or discuss any questions you may have with your physician.

How to “HIPAA”— Tip #10

.....
Look to the AMA for updates.

Summary of HHS’ New Guidance on the Privacy Rule

On December 4, the Office for Civil Rights at HHS released “Standards for Privacy of Individually Identifiable Health Information” (the “Guidance”). The purpose of the document is to provide practical assistance in implementing the privacy regulations created under HIPAA (the “Privacy Rule”).

The Guidance begins with a general overview that provides helpful general background on the Privacy Rule. The remainder of the document is divided into sections by key topics. These sections address Incidental Uses and Disclosures; Minimum Necessary; Personal Representatives; Business Associates; Uses and Disclosures for Treatment, Payment, and Health Care Operations; Marketing; Public Health; Research; Workers’ Compensation Laws; Government Access; and Miscellaneous Frequently Asked Questions.

Each section introduces the topic with a brief background and description of how the Privacy Rule works with respect to the specific topic. The “Frequently Asked Questions” (“FAQs”) that follow provide helpful insight regarding implementation of the Privacy Rule. Many of these FAQs address common concerns that physicians have raised. In addition, the Guidance provides specific answers to implementation issues such as who is a “business associate” and what is “marketing”. See the Summary of the Guidance below for a brief description of those sections that are like to be particularly helpful for physicians.

HHS acknowledges that the Guidance does not address all aspects of the Privacy Rule, but HHS indicates they will add segments in the future. In addition, HHS states that it will update the FAQs on an ongoing basis as new questions arise.

This document will serve as a useful resource for physicians as they implement the Privacy Rule. The examples are helpful and specific. The FAQs target many of the practical concerns that physicians have had about implementation of HIPAA. The Guidance can be found at <http://www.hhs.gov/ocr/hipaa/privacy.html> where physicians and their office staff can easily print and keep a copy as a resource.

General Overview

This section provides a brief overview of the Privacy Rule. The FAQs address the basics of the Privacy Rule, such as why the Privacy Rule is needed, and who is a covered entity. This section also provides a helpful summary of the major modifications to the Privacy Rule adopted on August 14, 2002.

Incidental Uses and Disclosures

This section explains that traditional methods of using protected health information are not likely to be severely restricted as a result of the Incidental Use and Disclosure provision in the Privacy Rule. It describes the balance between the need for privacy and the need for protecting efficiency and access in

delivering health care to patients. The FAQs provide examples of what reasonable and appropriate safeguards could include as required by the Privacy Rule. The FAQs also address how precautions to safeguard protected health information might work in emergency situations. In addition, the FAQs clarify common questions such as the use of faxes; placing patient charts in boxes outside of examination rooms; and other practices in the hospital setting where patients' names are typically displayed.

Minimum Necessary

This section explains the application of the Minimum Necessary Standard. For example, this section explains how physicians are not required to completely restructure existing workflow systems in order to meet the standard. Instead, HHS highlights the necessity of making reasonable adjustments to space and office operations to limit and minimize access to protected health information. The FAQs illustrate other simple ways to comply, such as locking file cabinets and providing additional passwords. The FAQs also explore how physicians can shape their policies and procedures in training situations to meet the standard.

Business Associates

This section clarifies some of the confusion surrounding business associates. It defines and provides examples of business associate relationships. It clarifies when a business associate contract is not required. The FAQs address concerns such as physicians' obligations with respect to protected health information held by their business associates. The FAQs provide guidance regarding physicians' potential for liability for the actions of their business associates.

Uses and Disclosures for Treatment, Payment and Health Operations

This section explains the final modifications to the Privacy Rule regarding consent. It clarifies why physicians may voluntarily choose to obtain their patient's consent. In addition, this section explains the implications of the definition of treatment, payment and health care operations. The FAQs offer helpful guidance on the differences between consent to use and disclose protected health information and informed consent for treatment. The FAQs also discuss the implications of use and disclosure of protected health information, authorization, ambulance services, common pharmacists' practices, professional liability insurance, and the use of debt collection agencies.

Notice of Privacy Practices

This section provides a through overview of the Notice of Privacy Practices, explaining its content, and when it should be provided. Electronic notice requirements are also discussed. The FAQs provide specific guidance about the notice in relation to other forms required by the Privacy Rule. The FAQs also provide examples such as notification to patients of changes to the notice and timing as when to provide the notice.