



# HIPAA

Health Insurance Portability  
and Accountability Act

## How to “HIPAA” – Top 10 Tips

.....

*Critical information to share with peers on how  
to comply with the Health Insurance Portability  
and Accountability Act.*

**[www.ama-assn.org/go/hipaa](http://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.	10/16/02 or 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.
Model Compliance Extension Plan for Transactions and Code Sets Standards	If a physician is not able to comply with the Transaction and Code Set rules by October 16, 2002, CMS requires the filing of a compliance plan no later than October 15, 2002. The form may be filed electronically or by mail, and the extension is automatic upon filing. If an extension is requested then compliance is required by October 16, 2003.	File no later than 10/15/02	If the physician is not in full compliance with the transaction and code set standard and does not submit a compliance plan by October 15, 2002, the Secretary of HHS has the discretion to exclude the physician from the Medicare program. Additional fines may be assessed.
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*	Business associates perform certain functions, activities, or services on behalf of the physician involving the use and/or disclosure of protected health information.  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.  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.	4/14/03 or 4/14/04	Physicians are not required to actively monitor the means by which the business associate carries out the safeguards of the contract.  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.  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.
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.	7/31/04	To be determined.

\*Modifications to these regulations are pending.

# How to “HIPAA”— Tip #2

---

*Know your compliance requirements.*

## **HIPAA: Who Must Comply?**

Physicians have less than six months to prepare for the first of several major deadlines under the Health Insurance Portability and Accountability Act (HIPAA). Many physician practices are working in earnest to comply with the federal law, but aren't entirely sure what is required of them. Many feel overwhelmed by the complexity of the task.

One question physicians frequently ask is, “We’re just a small practice, do we have to comply with HIPAA?” There is a lot of misinformation circulating about who must comply with HIPAA, and who is exempt. The following summary should help to clarify the issue.

### **Background**

The Administrative Simplification section of HIPAA has multiple parts - transactions standards/code sets; electronic signatures; security; privacy; and unique health “identifiers” for health plans, physicians, other health care providers, employers, and individuals. HIPAA requires the Secretary of the Department of Health and Human Services (HHS) to issue a set of interlocking regulations to implement each section. Physicians and other entities covered by HIPAA have two years to come into compliance with each final rule.

To date, only two HIPAA regulations are final and have established compliance dates - the Transactions Standards and the Privacy Rule. (The other rules have not yet been finalized and the individual identifier rule is on indefinite hold. See AMA HIPAA chart.) It is important to note that HIPAA permits modification of these rules yearly if determined appropriate, or if necessary for compliance. Modifications were recently proposed for the Privacy Rule and modifications for the Transactions Rule are expected at any time.

- Transactions Standards compliance deadline: October 16, 2002 or, for those who apply for an extension, October 16, 2003
- Privacy Rule compliance deadline: April 14, 2003

### **Who must comply with the HIPAA Standards?**

A physician must comply with HIPAA standards if the physician, a billing company or *other third party on behalf of a physician* transmits any health information in electronic form in connection with any of the following transactions:

- Health care claims or equivalent encounter information
- Health care payment and remittance advice
- Coordination of benefits
- Health care claim status
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments

- Referral certification and authorization
- First report of injury
- Health claims attachments
- Other transactions that the Secretary may prescribe by regulation (currently none of which the AMA is aware)

### **Who must submit Medicare claims electronically?**

A physician practice must submit Medicare claims electronically by October 16, 2003, unless the practice has less than 10 full-time employees. This is a new mandate from the Administrative Simplification Compliance Act passed in December 2001. The Centers for Medicare and Medicaid Services (CMS) will publish regulations regarding this requirement soon.

Many small physician offices hear this criteria and say, "Good, I have less than 10 full time employees, therefore I don't have to comply with HIPAA." Or they say, "I don't take Medicare patients so I don't have to comply with HIPAA." These are not accurate assumptions. If a physician practice submits any of the transactions listed above in electronic form, or a third party does so on its behalf, the practice must still comply with the HIPAA standards regardless of the size of the practice.

### **Who is exempt from the HIPAA Standards?**

A physician practice is exempt from the HIPAA standards only if:

- It does not submit electronic transactions (because it takes no forms of insurance or submits only paper or otherwise) and it does not accept Medicare patients.
- or -
- It accepts Medicare but has less than 10 full-time employees, and does not submit electronic transactions (because it takes no forms of insurance or submits only paper or otherwise).

©2002 Copyright. American Medical Association. All rights reserved.

[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 #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

---

*File your extension form for Transactions and Code Set Standards.*

### **HIPAA Alert: The first compliance date is almost here!**

**The October deadline for the Transactions and Code Sets Standards is quickly approaching...file your extension form today.**

#### **What:**

The Centers for Medicare and Medicaid Services (CMS) recently published a Extension Form (Model Compliance Plan) that covered entities (physicians, hospital, health plan, and clearinghouses) that submit claims electronically may use in requesting a one year extension for compliance with the Transaction and Code Set Standards.

#### **When:**

The deadline for submission of the compliance plan is October 16, 2002.

#### **How:**

To file a form, simply visit <http://cms.hhs.gov/hipaa/hipaa2/TCSFormInstructions.asp> or contact the Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore MD 21244-1850 for a paper form. If you file electronically you will receive an on-line confirmation number as acknowledgment of your extension. There is no approval process. Submitting the form is all that is necessary to obtain the extension.

#### **Why:**

- It is a simple process — there are no right or wrong answers.
- Filing for the extension will not preclude physicians from becoming compliant at anytime.
- It is anticipated that most health plans/insurers and other covered entities will also be asking for the extension. They will be seeking the extra time to be certain that their changes work with their provider communities.
- Physicians that are not compliant with the Transaction Standard requirements by October 2002 and have not filed for the year's extension can be excluded from the Medicare program.
- Some standards are changing which makes assuring compliance even more uncertain.

**File your form but keep working toward compliance!**

## 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:**

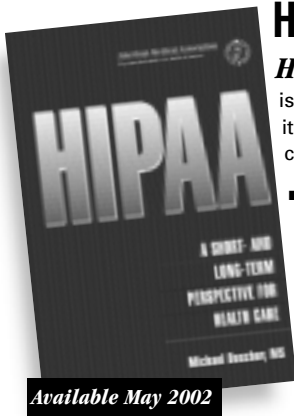
- Review of business associate contracts
- Review of employee contracts
- Gap analysis
- Risk assessment
- Implementation of compliance plans
- Ongoing monitoring
- HIPAA litigation

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

# How to "HIPAA"— Tip #6

Learn from trusted sources.

The **AMA** has answers to all your HIPAA questions



Available May 2002

## How does HIPAA affect me?

### ***HIPAA: A Short- and Long-Term Perspective for Health Care***

is a straightforward guide that provides a thorough review of the legislation including its genesis, supporters, intentions, and impacts. It then prepares you to take steps to comply by offering:

- model business agreements, sample assessment templates, and other valuable tools;
- guidance in assessing readiness for compliance and determining the risk of noncompliance; and
- insight to maximizing the benefits of investing in HIPAA compliance.

The content covers the day-to-day operational impacts of the security and privacy provisions and outlines how traditional and emerging health care information technologies can provide solutions to meet HIPAA and strategic e-commerce needs.

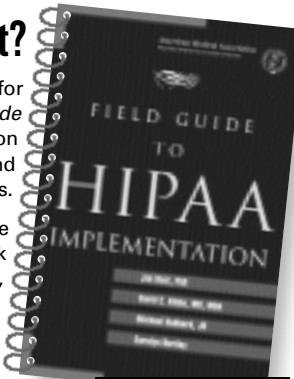
240 pages. Order #: OP319402BTH Price: \$79.95 AMA Member Price: \$74.95

## How do I become HIPAA compliant?

***Field Guide to HIPAA Implementation*** is a practical toolkit for those who want a seamless transition to HIPAA compliance. The *Field Guide* provides a wealth of resources to assist you through the implementation process, including troubleshooting tips, Web links, worksheets, and templates for forms and documents.

Timelines and to-do checklists help you track what needs to happen for the practice to achieve compliance, who should do the work, and when each task should be completed. And because the book was co-authored by a physician, an attorney, and an individual who helped write the transaction standards, you can be assured that the information is comprehensive and authoritative.

256 pages. Order #: OP319802BTH Price: \$139.95 AMA Member Price: \$134.95



Available July 2002

### **SPECIAL OFFER**

Order Both  
Books Today and  
Receive a  
15% Discount!

Get a detailed understanding of the HIPAA legislation and its impacts with ***HIPAA: A Short- and Long-Term Perspective for Health Care***, then use the ***Field Guide to HIPAA Implementation*** as your complete compliance resource.

**Order both books now and save more than \$30!**

Order #: OP319902BTH Price: ~~\$219.90~~ \$186 AMA Member Price: ~~\$209.90~~ \$178

To Order Call Toll Free 800 621-8335 or Fax 312 464-5600

AMA Members Only Call 800 262-3211 Order Online: [www.amapress.com](http://www.amapress.com)

VISA, MasterCard, American Express and Optima accepted. State sales tax and shipping/handling charges apply.  
Satisfaction guaranteed or return within 30 days for full refund.



American Medical Association  
Physicians dedicated to the health of America



For more HIPAA resources from the AMA, visit [www.ama-assn.org/go/hipaa](http://www.ama-assn.org/go/hipaa)

# How to “HIPAA”— Tip #7

---

*Separate fact from fiction.*

## The Top Fifteen Privacy Concerns

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.*

*\*HHS has proposed new regulatory language to clarify this issue.*

**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 my pharmacist from filling my prescription before I show up and sign that consent. Now, instead of having the prescription waiting for me, I’ll have to come to the pharmacy, sign a consent, and then wait around for hours while the prescription is filled.

**True!** *The Privacy Rule does not permit covered entities, including pharmacists, to use identifiable health information for treatment, payment, or health care operations without prior patient consent.*

*\*HHS has proposed new regulatory language to fix this problem.*

**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 reasonable 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.*

*\*HHS has proposed new regulatory language to clarify this issue.*

**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 (AMA)**

<http://www.ama-assn.org/go/hipaa>

*This section of the AMA web site offers HIPAA-related materials, tools and other valuable links.*

### **Centers for Medicare and Medicaid Services (CMS)—Model Compliance Form**

<http://cms.hhs.gov/hipaa/hipaa2/ascaform.asp>

*The model compliance/extension form can be found at this web site. This compliance/extension form must be submitted to CMS by October 16, 2002 if you will not be compliant with the HIPAA Electronic Health Care Transactions and Code Sets standards by that time.*

### **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](http://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/admsim/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.*

June 14, 2002

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. Regulations that more specifically articulate these obligations are in various stages of development.

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.

Attached is a sample letter that you may wish to give 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.

[on practice letterhead]

June 14, 2002

Dear Patient:

Physicians have always protected the confidentiality of health information by sealing medical records away in file cabinets and refusing to reveal your 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. Physicians have until April 14, 2003, 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 or other health care provider 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. We also take 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 officer 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 confidential 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 Officer at \_\_\_\_\_, or discuss any questions you may have with your physician.

# How to “HIPAA”— Tip #10

---

*Rely on the AMA for guidance.*

## **Modifications to HIPAA Privacy Rule (NPRM) AMA Comments - Executive Summary**

On March 27, 2002, the Department of Health and Human Services (HHS) published a proposed rule that would modify certain areas of the Privacy Rule pursuant to the Administrative Simplification portion of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Overall, the AMA believes the proposed modifications are a step forward. The following is a summary of the AMA’s comments to HHS regarding certain key proposed modifications.

### **Consent For Treatment, Payment, And Health Care Operations**

HHS proposes to make optional the previous requirement that health care providers obtain patients’ consent prior to using and disclosing information for treatment, payment, and health care operations. As proposed, covered entities (physicians, hospitals, other health care providers, health plans and clearinghouses) that choose to obtain consent could do so, with complete discretion in designing a process that works best for their practices. In addition, HHS proposes that health care providers make a good faith effort to obtain written acknowledgement from patients that they received a Notice of Privacy Practices. The AMA applauds HHS for its flexibility.

Under the proposed rule, patient information can be used for treatment, payment and healthcare operations without a written consent. HHS broadly defines healthcare operations (eg, underwriting and “business planning and development”). *The AMA urges HHS to narrow the definition of “health care operations” to only encompass those activities that are routine and critical for standard business operations, or that cannot be undertaken with de-identified information.*

### **Business Associates**

Because HIPAA only applies to health plans, health care providers and clearinghouses, the Privacy Rule requires these entities to protect patient information disclosed to any entity not covered by HIPAA through business associate contracts. Physicians, therefore, will be required to enter into written contracts with their business associates, ie: accountants, consultants, billing companies, etc. HHS proposes that existing written contracts with business associates would be “deemed” to be compliant with the Privacy Rule for up to one year following the compliance date of the Privacy Rule (April 14, 2003) – until the covered entity has renewed or modified the contract, or April 14, 2004, whichever is earlier.

The AMA appreciates that HHS has attempted to reduce some of the burdensome aspects of the business associate provisions. Yet, the proposal still leaves most of the burdens of the business associate provisions intact. These provisions would create unreasonable burdens, costs, and liabilities on physicians. *The AMA continues to argue that these provisions should be eliminated from the rule. Any extension of privacy rules to entities not covered by HIPAA must be achieved through new legislation.* In the alternative, HHS should completely rework

the provisions to eliminate or reduce many of the burdensome aspects, in accordance with previously suggested modifications the AMA, along with dozens of national medical specialty societies, sent to Secretary Thompson.

### **De-Identification Of Protected Health Information**

HHS' proposes that disclosure of a limited data set would be permitted – only for research, public health, and health care operations purposes. The limited data set would include the following identifiable information: admission, discharge and service dates; date of death; age (including age 90 or over); and five-digit zip code. In addition, HHS proposes that disclosure of the limited data set would be conditioned on the recipient's agreement: to limit the use of the data set; to limit who can use or receive the data; and not to re-identify the data or contact the patients. *The AMA strongly urges HHS to adopt such modifications in the final rule because they would provide a stronger incentive to use de-identified information.*

### **Marketing**

The AMA applauds HHS for proposing that all marketing would require patient authorization. Unfortunately, HHS has broadened the exceptions to the definition of marketing. *The AMA believes HHS should narrow the exceptions to include only those communications that are tailored to an individual and made by a health care provider or health plan.* If necessary, HHS should specifically clarify types of communications that would be permitted, such as refill reminders and preventive care services, while clarifying that purely promotional communications are not permitted. *At an absolute minimum, patients should be provided the opportunity to opt-out of any future communications that would fall under the exceptions to marketing.*

### **Administration Burdens**

The AMA's comments also stressed the continued need for HHS to reduce the administrative burdens of the Privacy Rule. Our comments highlighted:

- HHS should eliminate the privacy officer requirement for small physician practices.
- Small physician practices should not be required to document all of the policies and procedures mandated in the final rule.
- Physicians should be allowed to charge reasonable costs associated with some administrative requirements in the privacy rule.
- Compliance reviews of physician offices should be eliminated in the absence of specific complaints.

### **Parents as the Personal Representatives of Unemancipated Minors**

The proposed modifications would now allow physicians and other health care providers to overrule adolescents' privacy where State and other applicable law is silent and the parent is technically not the personal representative of the minor. While it is necessary and appropriate at times for a physician to inform parents or guardians of certain health problems facing a minor, the proposed modifications represent a loss for adolescents in determining who may have access to their protected health information. The AMA believes there should be no further erosion of the privacy protections for adolescents. To do so would seriously undermine efforts to ensure that minors will seek and receive necessary care.