February 17, 2000

Margaret A. Hamburg, MD
Assistant Secretary for Planning and Evaluation
United States Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201
Attn: Privacy-P, Room G-3222A

Subject: Comments on the proposed Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 through 164, 64 Fed. Reg. 59917 (November 3, 1999).

Dear Dr. Hamburg:

I am writing on behalf of the American Medical Association (AMA) and it members regarding the proposed rule on patient privacy issued by the Secretary pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The AMA appreciates the opportunity to provide our comments on the proposed rule.

## In General

The AMA acknowledges the considerable work by the Department of Health and Human Services (HHS) in attempting to create a regulation that meets the requirements of HIPAA and that embraces the Secretary's recommendations on patient privacy to the Congress two years ago. While the resulting proposed rule strives to accommodate both patient privacy and administrative simplification, the AMA believes that it falls far short on both counts. The complexity of the task, compounded by the inherent restrictions under HIPAA's limited grant of regulatory authority, have resulted in a proposed regulation that does not adequately protect patient confidentiality and privacy and that substantially and unacceptably increases administrative burdens for physicians. For these reasons, the AMA cannot support the proposed regulation in its current form.

Although our comment letter delves into significant detail in response to the proposed rule, the AMA's overarching concerns are as follows:

- that patients' confidential information could be disclosed without their consent for a broad array of purposes unrelated to the patient's individual treatment or payment and extending far beyond the necessary disclosures and uses patients would expect when they seek health care;

- that many holders of patient information who may misuse such information would not be held accountable under the proposed regulation, despite attempts to bring them within regulatory reach by compelling physicians and other covered entities to, in effect, "police" them;

- that physicians will be held liable for the uncontrollable misdeeds of their "business partners," although the physicians themselves are in compliance with the regulation's provisions;

- that the administrative burden and costs of implementing the proposed regulation have not been adequately calculated, and would have a disproportionate impact on small physician offices; and

- that the proposed rule contradicts the intention of its legislative directive under HIPAA to "simplify" health care administration and reduce costs, and does not improve patients' expectation of privacy in the health care system.

Under the proposed rule, the flow of information would not be limited to those individuals who should have access to confidential patient information in order to provide appropriate medical care. The AMA recognizes that the ability to use and manipulate computerized patient information presents an excellent opportunity to improve the medical care physicians and others on the health care team can provide. We caution the Secretary, however, that these opportunities for improvement will be lost if patients are afraid to provide important personal information to their physicians because of compromised confidentiality and privacy practices in the health care system.

We emphasize an important distinction here: the confidential relationship at stake is between the patient and his or her physician, other health care practitioner or health care team -- *not* between the patient and the health care system, including managed care organizations and entities with oversight functions. The physician and health care team are the guardians standing between patients and the unrestricted use and access to patients' private medical records. We believe that the preservation of patient trust and autonomy in a changing technological health care environment is imperative to continue high quality patient care that is expected in this country.

Personal health information is used by various entities in the health care delivery system, including hospitals and health plans, for purposes beyond direct treatment planning and claims payment. Many in the health care system and beyond believe that personally identifiable health information should be available for a vast array of seemingly compelling purposes without the explicit consent of the patient. Each of these entities argues it needs patient-identifiable health information to achieve its legitimate objective; most believe they do not need explicit patient consent to receive and use such information. That philosophy is reflected in the Secretary's proposed rule and preamble. It is a philosophy rejected by the AMA.

The AMA has continuously maintained that an expressed "need" for information does not confer a right. Patient consent continues to be a critical consideration in the use and disclosure of personally identifiable health information. Consistent with AMA's baseline philosophy regarding individual privacy rights, valid consent should be obtained, where possible, before personally identifiable health information is used for any purpose.

However, this is clearly not practical or even possible in some instances. In those situations in which patient consent is not feasible, either (a) the information should have identifying information stripped from it or (b) an objective, publicly-accountable entity must conclude that patient consent is not required after weighing the risks and benefits of the proposed use.[1] A local review board system has already been adopted successfully by several parties to the health care system, including physicians, some researchers, a few health plans, and others.

Some parties may reject this principle as too deferential to patients' rights at the expense of administrative feasibility. The AMA believes that this approach, explained in greater detail throughout our comment letter, properly balances the interests at stake. Furthermore, it is the right thing to do. At a time when the American public is looking to its leaders for a strong stand on patients' rights, any other policy fails patients, their families and their caregivers.

While we appreciate that the problems articulated above stem primarily from HIPAA's limited grant of authority to HHS, the AMA believes that the proposed regulation contains numerous deficiencies. Consequently, the AMA urges HHS to either (1) substantially revise the proposed regulation and reissue it as an interim final rule with the opportunity for comment, or (2) withdraw the proposed rule and issue a new NPRM.

## Specific Comments And Recommendations

In the event that the proposed regulation is not withdrawn, the AMA offers the following specific comments in order to bring this proposed regulation within a framework that will provide adequate protections for patient confidentiality and privacy until Congress revisits its limited grant of authority or enacts comprehensive legislation.

### Background: Need for privacy standards.

The AMA notes the Secretary's recognition that to "receive accurate and reliable diagnosis and treatment, patients must provide health care professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives."(59919) The preamble acknowledges that patients truly worry about their loss of confidentiality and privacy as health care increasingly moves from a paper-based information system to one that is electronic-based.

At the heart of "confidentiality" is the pledge by the physician not to divulge patients' private information to third parties without the patient's consent. In its Code of Medical Ethics, the AMA holds that "a physician shall… safeguard patient confidences within the constraints of the law." This core value of medical ethics is reiterated in the Code's *Fundamental Elements of the Patient-Physician Relationship*, where it is stated that "…the patient has the right to confidentiality. The physician should not reveal confidential communications or information without the consent of the patient, unless

[1] AMA Policy H-315.978, "Privacy and Confidentiality."

provided for by law or by the need to protect the welfare of the individual or the public interest."

Confidentiality lends itself to the establishment of a relationship based on trust, and maintaining the confidentiality of a patient's health information reinforces the notion of patient autonomy or control over decisions to disclose or retain information about himself or herself. When someone else proceeds to reveal confidential health information, control or patient autonomy has been taken away and trust is lost.

While confidentiality is a fundamental tenet in the ethical practice of medicine, confidentiality is not an absolute. In some instances, physicians must weigh whether to respect confidentiality against protecting the interests of others. This conflict is recognized in AMA policy and Ethical Opinions sanctioning breaches of confidentiality when "overriding social considerations," such as imminent harm to another or the outbreak of communicable disease, outweigh the individual's right to privacy."[2]

**Summary and purpose of the proposed rule.**

Here, as elsewhere in the proposed rule's preamble, the Secretary describes the pressing need for federal legislation "to establish comprehensive privacy standards for all those who pay and provide for health care, and those who receive information from them." (p.59923). The preamble repeatedly refers to the limited regulatory authority granted the Secretary by the Congress under the Health Information Portability and Accountability Act of 1996 (HIPAA) as a confounding factor, prohibiting the Secretary from proposing policies believed to be "more optimal." (p. 59923). Even in fulfilling her Congressional mandate to publish proposed regulations under HIPAA, the Secretary demonstrates a clear preference for legislative action and perhaps for action that has the effect of completely overruling her own regulation.

**Provisions of the proposed rule.**

**Applicability.**

Covered entities.

Although we recognize the Secretary's limited authority under HIPAA, the AMA is deeply concerned that the proposed regulation does not cover the entities that are most likely to wrongfully disclose and misuse confidential patient information. The rule does not regulate any secondary users of protected information, including employers, contractors, marketers, life insurers, public health officials, researchers, and law enforcement.

The AMA is also concerned that physicians who do not conduct electronic transactions would become subject to the proposed regulations if another entity using its records downstream "transmits health information in electronic form in connection with a

[2] AMA Ethical Opinion 5.05, "Confidentiality."

standard transaction on their behalf." (59927). Such application may raise problems determining whether a physician or other health care practitioner must comply with the proposed regulations.

If the proposed regulation provided an adequate level of protection for confidentiality and privacy, the AMA would support the proposed regulation's application to all health plans, health care clearinghouses, and health care providers who transmit health care information in any medium, whether or not in electronic form. But, in the proposed regulation's current form, the AMA cannot support such a broad definition.

Covered information.

The AMA finds deeply confusing the manner in which the NPRM explains what information is covered under the proposed regulation. According to the NPRM, "once protected health information is transmitted or maintained electronically, the protections afforded by this regulation would apply to the information in any form and continue to apply as the information is printed, discussed orally, or otherwise changed in form. It would also apply to the original paper version of information that is at some point transmitted electronically."

In effect, the privacy regulation could apply to health information in *any* form, including the original paper record from which the electronic data is ultimately derived. So while the regulation would technically apply only to health information that is transmitted electronically, this "backdraft" effect would suggest that *all* information – paper or electronic – would be subject to the standards, unless the information only and always stays in paper form.

A 1998 AMA survey of physicians found that more than nine out of ten (93%) physicians have access to a computer in their medical practice. Of those physicians who have access to a computer, 96% of those computers have modem capabilities and 78% have communications software for submitting claims. Therefore, in a majority of instances, it can be assumed that health information generally will not remain in paper form. Consequently, the AMA is informing its constituency that a prudent interpretation of the regulation would apply to all records regardless of form or medium, unless the physician is certain that the paper document will never be computerized and will never leave his or her office.

Despite this reality and educational effort, we believe that the NPRM's current explanation of what is covered will likely lead to widespread confusion on how to treat records that are perceived to be "mixed," i.e., containing both protected and unprotected information. The proposed regulation requests comment on "how best to protect information in mixed records, without creating unnecessary administrative burdens." It suggests – somewhat implausibly -- the possibility of developing a "'watermark' analogous to a copyright label, designating which written information is protected." (p. 59929). We do not believe there is any regulatory method of reliably protecting so-called "mixed" records. The AMA also certainly agrees with the HHS's acknowledgement that

the NPRM as it currently exists creates "awkward enforcement ambiguities," and suggests that HHS reconsider how it explains what information is covered.

In order to reduce anticipated administrative burdens for physicians and other covered entities, the AMA is inclined to support the approach, discussed in the preamble (59929), that all records should be covered under the same standard. We believe that the Secretary has the current authority under HIPAA to expand the definition of "covered information" to include all health information, regardless of its medium. Not only would such a construction reduce confusion among covered entities, it also would assure patients of an equally protective set of standards by which their health information would be handled.

However, AMA's support for such a construction would be contingent upon a revision of the proposed regulation that would provide an adequate level of protection for patient privacy and confidentiality. **In the proposed regulation's current form, the AMA supports the exemption of paper records that have never been, and will never be, reduced to electronic form.**

The Secretary also requests comment on whether HHS should draw on "other authorities to amplify the protections" of the proposed privacy standards (p. 59929). The AMA likely would support "drawing on other authorities" if indeed such action would result in more uniform protections. For example, if HHS could bring within regulatory reach all parties who hold individually identifiable information, instead of holding physicians and others accountable for their "business partners'" misuse of health information, the AMA may be supportive. However, without knowing which authorities HHS is suggesting drawing upon and to what end, we cannot offer a more definitive comment at this time.

<u>Interaction with other standards.</u>

The proposed rule notes that the privacy standards it sets forth "would be closely integrated with other standards that have been proposed under the HIPAA Administrative Simplification title. This is particularly true with respect to the proposed security standards published on August 12, 1998 (63 FR 43242)."

At the time of their initial publication, the AMA expressed strong opposition to the proposed Security Standards regulation. We concluded that the proposed rule flew in the face of its intended goal of "administrative simplification," and we urged that it be withdrawn in its entirety. Our concern at the time was that the proposed rule on security standards would impose such an excessive level of regulatory micro-management as to discourage physicians' offices from just such a desired transition.

In previous HIPAA NPRM comments we stated that harmonization is an essential component in implementing the HIPAA standards. The AMA believes that an orderly sequence of implementation is necessary for the goals of administrative simplification to be achieved. First and foremost, we believe that the enactment of comprehensive federal confidentiality legislation is the necessary and essential precursor and foundation for promulgation and implementation of federally regulated privacy and security standards.

**Definitions.**

Covered entity. (see comment under Applicability)

Health care clearinghouse.

**The AMA opposes the exemption of clearinghouses from a number of the provisions of the rule that would apply to other covered entities.** Regardless of the fact that clearinghouses may not deal directly with individuals, they deal directly with individually identifiable health information. If the clearinghouses are exempt from several of the provisions within the regulations, those exemptions should be clearly identified.

If a clearinghouse is to "be bound by their contracts with covered plans and providers," they should also be held accountable for and comply with the regulations regarding confidentiality and security requirements in instances where they are acting as a "switch" or a "trusted third-party." For example, a clearinghouse may have a contract directly with a "business partner" such as a physician or it may be possible that a clearinghouse will not have a contract with the physician but may have a contractual arrangement with the physician's vendor or billing services. Transactions may go through several entities or switches before actually reaching a clearinghouse. **Therefore, those entities that do not have a direct contractual arrangement with the physician should also be subject to compliance with the provisions and the penalties for a knowing misuse of individually identifiable information** (e.g., information being transmitted between two "trusted" business partners, between a business and a service provider or vendor, or between a business and a government or licensing organization).

In the future, with the use of the Internet and new technology there may be no "physical" contractual arrangements between the source of the patient data and the entities in the chain that receives and/or delivers the data through to its end point. The AMA believes that the clearinghouses and any trusted third-parties should comply with established security policies and technology solutions for governing the access and exchange of individually identifiable health information between individuals and organizations using Internet-based services for transactions (e.g., electronic mail, file transfers, hypertext transfers, and electronic data interchange). In addition, those entities should be subject to compliance with the provisions and the penalties for a knowing misuse of individually identifiable information.

Health care provider.

**The AMA approves of the consistency of using the definition of "health care provider" from HIPAA, and particularly supports the inclusion of health care professionals who provide services at schools or businesses.**

The Secretary requests comment on whether Internet pharmacies should be included in the definition of "health care provider." The AMA generally supports the availability of

the Internet to assist patients in obtaining prescription medicines as long as diagnostic and treatment decisions are made by physicians, and effective verification and security systems are in place to support appropriate patient information required in issuing a prescription. In the context of this proposed rule, it is essential that patient information remains secure and confidential during the transaction. If a "bricks and mortar" pharmacy is a covered entity under the rule, we see no reason why an Internet pharmacy should not also be covered. Other federal or state laws that may also regulate the operation of Internet pharmacies would be complementary, rather than exclusive.

Health information.

The AMA questions the omission of "researcher" from the list of those who create or receive information that "relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual." If information created or compiled by a school regarding the health status of its individual students could be labeled "health information," we fail to see how information compiled by a clinical researcher regarding an individual could elude the designation of "health information." **The AMA recommends the inclusion of "researcher" among the entities who create or maintain "health information."**

Health plan.

The subject of workers' compensation is complex and could be the subject for a separate rule addressing the rights and responsibilities of employers and their employees in the realm of privacy. The current proposed rule seemingly takes a "by" on this consequential issue by exempting workers' compensation more or less completely. We believe this is an inadequate response.

The fact that other forms of insurance with health components are also exempted is equally troubling to the AMA and, we believe, a poor public policy choice. Does the exclusion on property and casualty insurers from the scope of the rule mean that they can use and possibly market individually identifiable health information that their affiliated health insurance plan cannot? What are the barriers imposed? Does it matter to the individual which plan is paying his or her medical bills after an accident and should that individual's privacy protections be lesser depending on the source of benefits? **The AMA believes the answer is a firm "no," and recommends that all such coverages be included in the definition of "health plan."**

Transaction.

The AMA supports the development and use of national standards for electronic transactions. By increasing standardization and focusing on the readiness of third-party payers to engage in standardized electronic transactions, HIPAA and its resulting regulations can do much to spur substantial physician participation in electronic commerce.

We have long held that increased use of electronic financial and administrative transactions could increase the efficiency of physicians' practices as well as of the health care system overall. We, like others, have also identified a lack of national standards as a major bar to increased and cost-effective physician use of electronic data interchange (EDI) and other forms of electronic commerce. By specifying standards, and by "standardizing" these standards, EDI can be more attractive and useful to physicians, thereby accelerating the annual increases that we have seen in their use of EDI.

The AMA also supports web-based transactions *contingent upon* effective verification and security. However, the AMA believes that the data content must be equal to that required for the standards regardless of how the transaction occurs. Although much of today's EDI health care transaction business is conducted using a batch environment, web-based transactions are becoming very popular and will likely expand in the future. Batch transactions require submission of data elements in addition to the essential data content. Web-based transactions do not require the transmission of all the data elements in the proposed standards in order to satisfy the essential data content. Web-based transactions should not be considered a substitute for the proposed standard, but a supplement. Therefore, the AMA believes that for web-based transactions, a receiver should not be required to rebuild the transaction into the proposed standardized transaction for internal use, even though the data content that was received was equal to that required in the standard. To require the rebuilding of the transaction seems unnecessary and may stifle future technological innovations.

Business partner.

Since the Secretary's regulatory authority is currently limited to physicians, providers, health plans and health data clearinghouses, all other users of individually identifiable medical information in the health care system are *not* directly regulated by the proposed rule. The proposal identifies these secondary users as "business partners" of physicians and the other entities covered by the rule and they could only be held to the confidentiality standards of the regulation through contracts with the covered entities, such as physicians. A physician group, for example, could then be held accountable for prohibited activity by its business partners, even if the group had no knowledge or control over the practices of its business partner. The AMA objects to these provisions because they present the potential for significant liability for physicians who, themselves, are complying with the regulation's requirements. [See also discussion on Application to Business Partners]

If the final regulation retains the concept of the "business partner," the AMA believes that the term's definition should be expanded to include "trusted" business partners with appropriate verification techniques and secure online communication in place such as network partners, out-sourced clinical services, alliance hospitals, etc. that have a legitimate need to access clinical data. Many transactions in the future will be sent via the Internet with secure encryption and digital credentials to identify the sender/receiver. The rule should make provision for these types of relationships.

Designated record set.

The AMA believes that the definition of a designated record set in the proposed rule could be problematic, in that it describes records "used by the covered entity to make *decisions* about the individual." As the preamble notes, the "designated record set" would include not only the predictable medical charts, billing and enrollment records, but would also embrace other communications or tracking systems regarding the individual patient or enrollee. While we appreciate the exclusion of back-up files and similar records, we nevertheless believe that the volume of less systematized communication regarding a patient or enrollee within a covered entity could be significant, and making it available to meet the access requirements of the proposed regulation overly burdensome. Perhaps there might be some way to distinguish a first and second tier of records, such that the basic access request would provide the non-duplicative systematized records used to make decisions and provide notice that the other information would be available, if needed. Such an approach may create a lesser administrative burden, and could be supported as long as the privacy protections accorded each tier of information would be equal.

Health care operations (Sections 160.103) (See also Section 164.504, "Treatment, Payment, and Health Care Operation")

The AMA is deeply concerned and surprised by the breadth of activities HHS believes to be "compatible with and directly related to" treatment and payment. We recognize that patients have a reasonable expectation that the nature of treatment rendered by their physician or other health care practitioner will be revealed to their health plan or other insurer for purposes of payment. However, patients would not expect, nor would they welcome, unauthorized access to health information disclosed in the context of a confidential relationship for the wide range of purposes HHS believes to be somehow "compatible with and directly related" to treatment or payment.

First, many of the activities listed in the NPRM under the definition of "health care operations," for example "quality assessment and improvement," clearly are NOT "compatible with and directly related to treatment and payment" as the proposed regulation suggests. Though arguably some of the activities may be related to treatment and payment in the aggregate, several of the activities described in the NPRM clearly are not related to any one medical service or payment thereof. **We believe the measure of whether an activity is "compatible with and directly related to" treatment or payment would be whether the purpose of the activity was to specifically and directly benefit that particular patient.** Advantages to the patient or enrollee population generally might eventually accrue to the individual patient, but are not directly intended for the medical benefit of a specific and unique individual.

The diversity of proposed uses advocated by various groups illustrates the inherent difficulty in addressing these evolving functions within any static legislative or regulatory definition. It also suggests the implausibility of reaching consensus on which functions

are appropriate and which are not. Health care systems must be dynamic and flexible to compete in today's economy. It would be foolhardy to expect that the current list of uses for health information will remain static. The Secretary notes this when she states that "the health care industry is changing and that these categories [of "health care operations"], though broad, may need to be modified to reflect different conditions in the future." (P. 59934) Why not create a system that accepts this fact and builds in enough flexibility, while continuing to place patients' rights to control their information in a preeminent role?

The AMA believes the issue should be re-framed and that it is unnecessary for a single federal law or regulation to create an immutable, one-size-fits-all scheme. **We recommend application of the controlling rule iterated previously: valid consent should be obtained before personally identifiable health information is used for any purpose. For those many functions or circumstances for which patient consent is not feasible, the information would either have to be de-identified to be used, or the decision regarding its use without patient consent would be made by an objective, publicly-accountable process that weighs the risks against the benefits of the proposed use**.

**The AMA believes that operational uses of personally identifiable health information, as well as research projects that fall outside the purview of an IRB process, should be subject to review by privacy boards, as described by the Secretary in the Research provisions of the proposed rule, and should be held to the same standards that apply to Institutional Review Boards.** Such an approach honors the rights of the individual and the primacy of patient consent, which the Secretary herself has described as "generally more protective of privacy interests than the lack of such authorization." (p. 59997) Yet it also does not create an unduly restrictive barrier to patient information for legitimate uses and creates a mechanism for those seeking medical records to establish their credibility and legitimacy. In short, it creates accountability. [See discussion under Research provision.]

The privacy board also creates an incentive to de-identify health information at the earliest possible opportunity, also consistent with the Secretary's expressed intent of the proposed rule. We fail to see why many of the activities termed "health care operations" could not be carried out using de-identified patient information. AMA believes that if a covered entity has a legitimate need for identified health information, for purposes other than treatment or payment, other truly related purpose, or clearly defined public health benefit, the entity should be required to obtain consent to use the information. If consent is neither practical nor possible, we would advocate for a publicly accountable, objective balancing mechanism to make such decisions on behalf of the patients, weighing the relative risks and benefits, as well as the security measure in place to assure the confidential handling of protected health information.

<u>Health oversight agency.</u>

The proposed regulation defines a health oversight agency broadly as a "public agency authorized by law to conduct oversight activities in relation to the health care system, a government program for which health information is relevant to determine beneficiary eligibility or a government regulatory program for which health information is necessary for determining compliance with standards." (59958) Examples of agencies included are state insurance commissioners, state health professional licensure agencies, the Office of Inspectors General of federal agencies, the Department of Justice, State Medicaid fraud units, Defense Criminal Investigative Services, the Pension and Welfare Benefit Administration, the HHS Office for Civil Rights, the FDA, the Social Security Administration, the Department of Education, the Occupational Health and Safety Administration, and the Environmental Protection Agency.

However, private accreditation organizations such as the Joint Commission on Accreditation of Health Care Organizations (JCAHO) would not be included in the definition of a "health oversight agency." Only governmental or private entities that contract with the government to conduct oversight activities would be included.

The AMA is concerned that many governmental agencies do not have clearly defined oversight duties in the health care arena. We believe that the definition's sweeping inclusion of virtually all government agencies that may have any connection, albeit remote, to health care may result in widespread fishing expeditions for confidential patient information. Even more troubling, is that the proposed regulation promotes such access knowing that there are few safeguards in place to protect against the government's wrongful disclosure or use. As we discuss later in this document, the AMA strenuously objects to the seemingly unfettered and unauthorized access governmental agencies will be accorded under the proposed regulation as it is current drafted.

Individual.

The Secretary would include in her definition of individual a person with "power of attorney." The AMA is concerned that under the proposed regulation, legal representatives with "power of attorney" for matters unrelated to health care would be given unauthorized access to confidential medical records. In fact, the proposed regulation discusses this situation, and concludes that it would be appropriate to allow health plans and providers to disclose confidential information to such persons without patient authorization. We cannot support this approach, and **recommend that the Secretary limit disclosure without authorization to those individuals or legal representatives who are given power of attorney over issues directly related to health care.**

We would also like to share a concern voiced by the transplant community regarding the definition of "individual." Their request is that, with respect to deceased persons, next-of-kin (as defined by applicable law) should be permitted to represent the decedent, along with the executor, administrator, of other person authorized under applicable law to act on behalf of the decedent's estate. Their concern is that the definition should not inadvertently preclude information from flowing with organs in the procurement process.

Individually identifiable health information

We agree with the Secretary's decision to reject defining non-identifiable information to mean "anonymous." However, we do not believe the correct balance has been struck in Section 164.506(d), regarding the de-identification of information. Although the Secretary's intent is to encourage de-identification of records, the complexity and administrative burden of this section has the perverse result of *dis*couraging de-identification. [See discussion at General Rules: Creation of De-identified Information]

Also, due to its limited applicability under HIPAA to health care providers, health plans and health care clearinghouses, the proposed rule does not prohibit subsequent recipients of "de-identified" information from re-identifying it. This is another fundamental flaw in the proposed rule resulting from the limited grant of authority and scope under HIPAA.

Law enforcement official.

The proposed regulation defines a "law enforcement official" broadly as an officer "empowered by law to conduct an investigation or official proceeding inquiring into a violation of, or failure to comply with any law…." Seemingly, under this definition, many government officials (even those without health care oversight duties) would be able to access records without patient consent. Although we understand reasons why the Secretary might feel the need to broadly define "law enforcement officials," we remain concerned about the proposed regulation's lack of safeguards to prevent government agencies from wrongfully disclosing or misusing confidential and private health information.

Payment.

The AMA shares the Secretary's concern that disclosures for payment may routinely result in disclosure of protected health information to employers and other non-covered entities. The proposed regulation recognizes that "employers are paying for health care in many cases, and … they may need access to claims and other information for the purposes of negotiating rates, quality improvement and auditing their plans and claims administrators." While we acknowledge the legitimate uses to which an employer might put such information, the AMA believes that many of these functions should be performed with de-identified information and that employers should not be permitted to access their employees' individually identifiable confidential medical information without the employee's authorization.

**Therefore, the AMA would support one of the Secretary's approaches considered to resolve the issue of employer access, i.e., prohibiting disclosures to employers without individual authorization**. The AMA believes that employers should be barred from unauthorized access to identifiable medical information. In general, knowledge of sensitive facts could form the basis of adverse decisions against individuals. Many, if not most, legitimate employer activities regarding improving health care for its employees

may be conducted with de-identified and aggregate data, for which consent would not be required.

Protected health information.

The AMA is not comfortable with the proposed regulation's definition of "protected health information," which means "individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form." We point out that under principles of medical ethics, little distinction can be made between sources of information based on mode of transmission, electronic or not. That is, with regard to disclosure and authorization to disclose protected health information, the source of the information is not determinative of its protected status.

Psychotherapy notes.

Effective medical diagnosis requires patients to be willing to reveal details about their most personal behavior and physical and psychological conditions to their physicians and other health care practitioners. The "imperative need for confidence and trust" between patient and practitioner has been recognized by the U.S. Supreme Court in the psychiatric context. *Jaffee v. Redmond*, 518 U.S. 1, 15-16 (1996). However, the need for confidentiality and trust extends well beyond psychiatry.

The AMA believes that there is a critical need to protect all individually identifiable health information regardless of its context. The fact that a special carve-out is needed in order for the proposed regulation to be consistent with the U.S. Supreme Court's ruling, demonstrates that the proposed regulation, as currently drafted, is an inadequate vehicle to provide much needed protection against inappropriate disclosure and misuse of confidential health information. If the proposed regulation provided a reasonable level of protection for individually identifiable health information, a carve-out for psychotherapy notes would not be necessary.

Research information unrelated to treatment.

This definition is problematic, in that it is unclear exactly how such information is distinguishable from "research" information, particularly over time. What is the effect on records when a treatment becomes medically verified? Are protections retrospective? If the distinction being made is one between archival and clinical records, it would seem to make an equally precarious and ethically unacceptable distinction between treatment patients receive when participating in a clinical trial and when receiving "regular" care. We understand that others interpret this definition to address genetic information, a reading we find hard to follow. However, the confusion points up that the term is poorly defined in the regulation and further muddied in the preamble's narrative. **We recommend eliminating the distinction completely. Patient protections should not be dependent on whether a health plan will pay for certain care.**

Treatment.

**The definition of "treatment," which as proposed seemingly would include cost containment mechanisms such as case and disease management, is too broad. The AMA suggests that the definition be narrowed. For example, "treatment" could be defined simply as "the provision of or coordination of health care services among physicians or other licensed or certified health care practitioners or providers."**

Such a definition would eliminate all references to coordination of care with third party payors, which employ coordination mechanisms (such as disease management and case management) primarily for the purpose of managing costs, not treating patients. And, though the AMA recognizes that there are numerous times when third party payors enter the realm of making "treatment" decisions, at the current time many health plans (particularly ERISA plans) maintain that they do not make treatment decisions, and argue against assuming liability for making treatment decisions. They cannot have it both ways.

The term "disease management" is undefined in the proposed rule; however, its proponents define it as a broad-ranging set of "multidisciplinary" initiatives to "continuously evaluate clinical, humanistic and economic outcomes with the goal of improving overall health."[3] This all-encompassing definition would seem to justify almost any information use under the proposed rule and we believe it is a significant and potentially harmful loophole that must be closed.

The danger of equating information disclosures for "disease management" with disclosures for treatment is not a theoretical one, as anyone knows who has received mailings at home for an alternate, competing medication after having filled a prescription at the pharmacy. If the true motive of its proponents is to improve individuals' care, then they should not object to coordinating all disease management activities through the individual's physician. If, however, the purpose is rather ultimately to market protected health information to commercial entities or employers, then the proponents will eschew physician participation and seek to directly influence the patient. **The AMA opposes any "disease management" language in the proposed rule that is not qualified by requiring the coordination and cooperation of the individual's physician.** An example of such a qualification in current law is found in California's "Confidentiality of Medical Information Act, which allows disclosure for chronic disease management programs to plans and contractors of plans to monitor or administer enrollees' care for a covered benefit, "provided that the disease management services and care are authorized by a treating physician."[4]

---

[3] From the Disease Management Association of America definition of "disease management": "a multidisciplinary, continuum-based approach to health care delivery that proactively identifies populations with, or at risk for, established medical conditions that supports the physician/patient relationship and plan of care; emphasizes the prevention of exacerbations and complications utilizing cost-effective evidence-based practice guidelines and patient empowerment strategies such as self-management education; and continuously evaluates clinical, humanistic and economic outcomes with the goal of improving overall health."

[4] Cal. Civil Code Section 56.10(c)(17), as added by 1999 Cal. Stats. Ch. 526, sec. 2.

Clearly, there are opportunities for disease management programs to assist patients. **Patients should have the right to consent to – or refuse – participation in disease management programs offered by providers and plans.** It is not anticipated that this would impose any significant additional burden; plans, for instance, already have a variety of interactions with enrollees, including the initial and annual enrollment process. **If the disease management activity is conducted by a secondary organization or contractor, the individual should have notice of this in the consent form. If the information is going to be used for any marketing or employment purposes, this should be explicitly noted in the consent form. And in no way should an individual's enrollment or costs be affected by his or her decision to not participate in a plan's disease management program.**

The AMA is also taken aback at the Secretary's intention, articulated in the preamble, that the "right to use and disclose protected health information be interpreted to apply for treatment and payment of *all* individuals." (emphasis added) (p. 59940) The Secretary provides two examples, neither of which are acceptable options under AMA's Code of Ethics. The first suggests that in the course of providing care to a single patient, a physician can randomly access the files of other patients with similar conditions, even if that physician has no relationship with the other patients. The second describes a situation where a physician, according to the Secretary, would be able to access the records of several people in the same family or living in the same household (e.g., roommates) to assist in the diagnosis of contagious conditions or that could arise from a common environmental factor.

For clinical purposes, AMA policy and Code of Ethics require that "physicians or other health care professionals not directly involved in a patient's care who wish to gain access to confidential medical information must obtain explicit patient consent before doing so. Informal case consultations that involve the disclosure of detailed medical information are appropriate in the absence of consent only if the patient cannot be identified from the information"[5] The wearing of a white lab coat is not a "get in for free" ticket. Such a basic misunderstanding of physicians' ethical obligations and the character of the patient-physician relationship cannot go unnoted here.

We are further appalled to read the Secretary's expanded construct of this idea of universal access for health plans or providers who could "use the protected health information of a number of enrollees to develop treatment protocols, practice guidelines, or assess quality of care," apparently with no thought to patient consent. (p. 59940) This faulty line of reasoning may explain what was before puzzling to us: the Secretary believes that since physicians have universal free access to confidential patient information, then so must other entities. The premise is wrong and so is the conclusion.

**General rules.**

[5] AMA Policy H-140.927, "Access to Medical Records by Non-Treating Medical Staff."

The proposed regulation seemingly is more concerned with facilitating the ease of information flow for the broadly defined purposes of treatment, payment, and health care operations than it is with protecting patients' confidentiality and privacy interests. AMA's policy states that "[c]onflicts between a patient's right to privacy and a third party's need to know should be resolved in favor of patient privacy. (H-140.989). In the AMA's view, the "general rule" should begin with preserving confidentiality and privacy and allowing disclosure only when it is ethically and legally justified.

Though, at first blush the proposed regulation's "general rules" seem to reflect this view, as broad definitions and interpretations of the regulation's more specific provisions are incorporated, clearly the proposed regulation does not place protecting patient interests first.

Furthermore, we agree with the Secretary's approach to provide a similar level of protection for all health information, not just sensitive health information. However, the proposed regulation's extremely low level of protection unfortunately encourages the need for carve-outs for sensitive information, which are accorded little protection under the regulation in its current form.

**Use and Disclosure for Treatment, Payment, and Health Care Operations (Section 164.506(a))**

We agree with the *intent* of the Secretary's proposal to make the exchange of protected health information relatively easy for health care purposes and more difficult for purposes other than health care. However, despite the requirement that only the minimum amount of information necessary be disclosed, we are concerned that as a consequence of the breadth of the disclosures authorized under the NPRM, patients may be reluctant to share confidential information with their physicians.

The Secretary notes, and the AMA agrees, that individuals generally do not recognize that their information may be used for a multitude of purposes beyond their individual care and payment for that care. This fact underlies the AMA's advocacy for a consent requirement for *most* uses of an individual's private health information. The Secretary herself acknowledges in the preamble (p. 59997) that "[w]e consider individual authorization generally to be more protective of privacy interests than the lack of such authorization…" and so are disappointed that the proposed rule does not do more to endorse an authorization approach.

Minimum necessary use and disclosure

The proposed rule would require each physician office to establish a "minimum necessary" standard, which involves establishing and documenting procedures and policies to limit access and training staff. Each request for disclosure would be required to be reviewed on its own merits. There is much gray area between what is "necessary" information for medical reasons and what is too much disclosure such that the standard is violated. What is "reasonable" is highly subjective and compounds the problem of cost

estimation. In addition, this requirement, in its current iteration, unfairly puts the onus largely on physicians to establish the motives and needs of various record requesters.

We believe that the current "minimum necessary" standard, while of laudable intent, may be unworkable. **To achieve the same goal of precluding wholesale transfers of complete medical records when only a small portion is pertinent to the patient's current treatment, we recommend that the rule adopt a provision similar to that proposed in a bill being considered by the Massachusetts legislature. Rather than requiring that the "minimum amount necessary be disclosed" in response to record requests, the rule should adopt a requirement for *requester* to make the "minimum necessary demand."** While physicians could certainly engage the requester in a dialogue regarding what specific information might be needed in any given instance, the liability would be on the requester for seeking prohibited information, rather than on the physician for not adequately divining the motivations of the requester. We believe this is a fairer and less administratively cumbersome method of achieving our mutual goal of protecting patients' information.

Under this approach, we believe physicians would retain their role as ultimate protector of a patient's record and would be able to challenge demands that, in their professional judgment, were excessive. Retaining this ability to challenge overly broad requests would keep the system fair and provide for some internal tension to assure that the standard was honored, assuaging some concerns that there would be no practical way to enforce the proposed rule's current standard. It would accrue to any requester's benefit, then, in substantiating their request, to describe with great specificity the intended scope and purpose to which the requested information is to be put. While we understand that such a balance might not be possible under the current parameters of the proposed rule, given that the rule may only directly regulate the activity of "covered entities," we nevertheless believe that such an approach should be the ultimate goal.

**In certain instances, physicians should also be permitted under the rule to disclose a summary of the record, in conformance with the "minimum information" standard, rather than the full record itself.** While this obviously would not be the preferred option in many instances, we nevertheless believe that the option should be preserved by explicit inclusion in the proposed rule.

**On the question of scope, we also question why the "minimum necessary" standard would not apply to disclosures allowed under Section 164.510, for purposes such as health oversight, judicial and administrative proceedings, law enforcement, research, and others.** While the scope of authority granted the Secretary under HIPAA would not currently permit imposition of a "minimum necessary demand" standard, as recommended above, on non-covered entities, we believe that a comprehensive federal approach should pursue exactly such a requirement. A "minimum necessary demand" standard would also eliminate any potential conflict of interest in situations where information sought for investigative or enforcement purposes might be the subject of a requested disclosure. This underlines the importance of retaining physicians' ability to

challenge requests, as articulated in many States' laws of civil procedure permitting a physician to move a court to limit or completely quash an inappropriate request.

**Lastly, the exceptions to the "minimum necessary" standard in Section 164.506(b)(1) should be modified in (iv) to read:**

> **"(iv) Made by a covered health care provider to a covered health plan, when the information is requested for audit ~~and related purposes~~ <u>of that plan's enrollees' records only.</u>**

"Related purposes" is undefined in the regulation and should be eliminated. If the purpose is related closely enough to the audit function, it will be allowed as a necessary element of the audit; otherwise, it should not provide a "backdoor" to other marginally related purposes. Secondly, the health plan's relationship is with its own enrollees in a treating physician's practice. Even under the rubric of performing "health care operations," health plans do not have the permission of the physician's patients enrolled in <u>other</u> health plans to access their individually identifiable information without their express consent. Therefore, the AMA urges a modification of this standard to accurately reflect the patients' [relationships with each covered entity and the rights and obligations that flow from that relationship. ]

<u>Right to Request Restrictions on Uses and Disclosures. (Sec. 164.506(c))</u>

The proposed rule would permit individuals to request that the use and disclosures of their protected health information be restricted for purposes of treatment, payment and health care operations. If the covered entity agreed to the restrictions, the covered entity could not use or disclose the information for treatment, payment, or health care operations in ways that would be inconsistent with the agreed restriction.

At first blush, the ability for individuals to request restrictions on disclosures and use of their information for purposes of treatment, payment and health care operations appears to diffuse the criticism that individual authorization would no longer be required under the proposed rule for these purposes. A more careful analysis reveals this provision to be an unworkable "consolation prize" for patients who have had their right to consent taken away from them by government fiat.

In addition, individuals would have no right to request restrictions on disclosures or uses made without their authorization under Section 164.510. Thus, for judicial and administrative proceedings, for example, the individual would not have an opportunity to limit the amount of information disclosed if it was requested *without* benefit of a court order. **This deficiency might be repaired by requiring that requests for judicial or administrative proceedings *must* be accompanied by a court order limiting the amount of information to be disclosed and providing the individual with an opportunity to challenge that request.** [See comments under Judicial and Administrative Proceedings]

This same criticism applies to instances where information is requested for law enforcement purposes under Section 164.510. This is particularly true in situations where legitimate health oversight activities evolve into law enforcement actions.

Also under the current language of the proposed rule, individuals would have no right to request restrictions for disclosures to governmental health data systems, under Section 164.510(g). Thus, individuals would have no say whatsoever in keeping the entirety of their personal medical information out of governmental health data systems. The unfortunate conclusion patients might draw from this fact is that they are better off not seeking medical care for sensitive conditions. [See comments under Governmental Health Data Systems]

This makes the case for a consent requirement for those activities categorized under the proposed rule as "health care operations." If this right were expanded to restrict all uses and disclosures, patients would retain control over their health information. Rather than being asked to authorize specific uses and disclosures, patients could pre-determine those uses and disclosures that are compatible with their preferences and values. Re-enforcing patient autonomy is this manner would be in greater accordance with the principles of confidentiality espoused by the AMA in the Code of Medical Ethics.

In addition to its ethical flaws, we believe that offering a right to restrict presents the potential to drive a wedge between patients who want to impose further restrictions and providers who cannot agree to such arrangements due to the overwhelming administrative burdens and potential liability that such individual arrangements would entail. Ironically, we believe that the inclusion of the "right to restrict" provision points up the flawed framework of the proposed rule and ultimately makes the case for a consent requirement for all purposes.

**If the Secretary chooses to adopt this "right to request restrictions" approach in which an individual can request restriction on disclosures and uses of their information, several modifications must be made to make the provision meaningful:**

- Individuals must be able to request such restrictions from their health plan, as well as from their physician or health care provider (for example several individuals may be insured under a family plan, and their privacy needs may differ from the main insured's);
- The rights to request restrictions must extend to certain disclosures and uses currently permitted under the proposed rule without the individual's authorization (certain provisions of Section 164.510, especially next of kin, judicial and administrative proceedings, law enforcement, and governmental health data systems); and
- The right to restrict must not be conditional on the physician's or health care provider's acceptance when the individual "self-pays." However, such a provision must be conditioned on the physician's ability to limit his or her liability in cases where the patient does not want information shared for treatment purposes (this should make the case for why consent should be required for anything other than treatment or payment. For all but self-pay cases, though, the physician should have

should have the right to deny the request for restriction because he or she is best situated to evaluate whether it would unacceptably compromise care).

- Any restrictions should flow with the information to which it pertains, so that subsequent holders/users are bound by the restriction. The physician already has to notify subsequent holders of the restriction (Section 164.506(c)(2)(iv)), so the additional administrative burden on physicians would be seemingly minimal.

Creation of de-identified information.

The AMA favors any provisions of the rule that would have the effect of creating incentives to "de-identify" medical information. We are pleased that the Secretary, in the proposed rule's preamble, has noted the importance of creating such incentives. However, Section 164.506(d), apparently intended to provide guidance in de-identifying records, actually would create a *disincentive* to de-identify information. It articulates nineteen different characteristics or fields that would need to be removed from a medical record before the record could be considered de-identified.

Aside from the tremendous administrative burden this would create for any institution or entity, some of the characteristics or fields of information to be deleted would make the record completely useless for almost any research purpose. For example, the medical record number, health plan beneficiary number, account number and certificate or license number would all have to be excluded from a patient's file in order to comply with the rule. This would seem to preclude any cross-referencing of records, *even if those records had no other identifying information in them, save for these numbers.* Such numbers do not identify individuals unless the numbers are linked to a cross-index that includes names or more obvious identifiers.

**The AMA believes it would make much more sense to dramatically pare down the list of characteristics considered to be "identifying," and add a prohibition of the unauthorized *linking* of anonymous data with other lists that would reveal the identity of the individual. The linking for the purpose of identifying an otherwise unidentified individual would be a violation of the regulation, equivalent to the disclosure of identifiable information.** This "linking" prohibition would be in addition to the prohibition, in 164.506(d)(1)(i), of disclosure of keys or other devises to enable decoding or "re-identifying" de-identified information.

**In addition, the AMA recommends that Section 164.506(d)(2)(ii)(B), regarding Implementation Standards, be completely deleted.** The current language requires that, in addition to removing some 19 different potential identifying factors from a medical record, the physician must *also* divine the identity of "*any* anticipated recipient" and how that recipient "could use the information, alone *or in combination with other information*, to identify and individual." (emphasis added) As has been pointed out in oft-cited research on the subject[6] it is a complex and near-impossible task to completely protect "anonymous" individual records from cross-indexers eager to seek out the individual's

[6] Latanya Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality," 25 *Journal of Law, Medicine & Ethics* 98 (1997).

identity. It is unacceptable to require such omniscience from physicians or other covered entities.

We believe our recommendation to revise the list of "identifiers" to be removed from records, combined with an explicit prohibition against "linking" or re-identifying without authorization, would provide entities with a greater incentive to de-identify records, while holding the inevitable wrongdoers properly accountable.

Application to business partners.*(164.506(e))*

The AMA strongly objects to the proposed rule's approach of holding physicians and other covered entities responsible for certain violations of the rule's requirements by their business partners. We appreciate the limitations inherent in the Congressional grant of authority under HIPAA that constrains the Secretary from directly regulating secondary and "downstream" users of individually identifiable health information. The AMA also agrees with the Secretary that these users should be brought under the terms of comprehensive privacy rules. **We oppose, however, the contrived extension of the scope of the Secretary's authority through the "business partners" provisions of the proposed rule.**

Although covered entities can articulate their expectations for patient privacy in a contract with business partners, it is a fact that covered entities cannot control all acts of their business partners. Physicians and other covered entities would be required to act as regulatory deputies on behalf of the Department, in seeking oversight and compliance by business partners. Covered entities often have multiple contractual relationships, significantly complicating the "policing" role the proposed rule obliges them to play. It is unclear how frequent or detailed the covered entity's oversight of its business partners would be to be considered "reasonable."

As a matter of fairness, the proposal fails. While covered entities are subject to the full weight of enforcement and sanctions under the regulation for the prohibited acts of their business partners, the business partners would stand to lose far less -- at most, their contract with the covered entity and possible damages in any subsequent civil suit filed by the covered entity.

Physicians and covered entities would be subject to an array of both foreseeable and unforeseeable costs to comply with the proposed rule. All existing contracts with each business partner would need to be rewritten and possibly renegotiated. In addition to the multiple contractual provisions required by the proposed rule, it is expected that covered entities would certainly want to negotiate liability and indemnification clauses. In order to comply with the contract terms, it is anticipated that some vendors would renegotiate their contract price with covered entities.

Another element of the "business partners" provision that has not been considered by the Secretary is the potential cost to covered entities for assuming the enforcement responsibilities of the Department, as well as litigation costs for pursuing restitution from

business partners whose conduct has placed the covered entity, through no fault of its own, at risk of regulatory non-compliance. In sum, we believe the financial implications for physician compliance could be substantial under the "business partner" provisions of the proposed regulation.

Another mandated contract term that requires revising for real-world application is in Section 164.506(e)(2)(H), in which the business partner would be required, at the termination of the contract, to return or destroy all protected health information received from the covered entity, retaining no copies of the information. Collateral obligations of the business partner may demand that it maintain some of this information, particularly for audit and oversight purposes. Yet in the absence of a continuing contract with the covered entity, the proposed rule is unclear as to what protections might still attach to the information.

The proposed rule creates unnecessary complexity by characterizing covered entities that do business with other covered entities as "business partners." Physicians have numerous contractual agreements with other "covered entities," and it is difficult to untangle relative obligations under the current construction. For example, if a physician is an independent contractor with a hospital, who is the "covered entity" and who is the "business partner"? What if that physician is a member of a physicians' group that has a contract with a hospital?

**Since all covered entities' privacy practices are regulated under the proposed rule, it would make sense to add a rule of construction that no covered entity can be a "business partner" under the regulation.** This construction would also require the deletion of the provision in the current proposal whereby health data clearinghouses are sometimes exempted from obligations as a "covered entity." Here, as throughout the proposed rule, simpler would be better.

**We also support the carve-out to the contracting requirement for consultations and referrals.** We believe this provision can be further strengthened to permit the maximum access for treatment purposes, as long as the definition of "treatment" is circumscribed in such a way as to include only those activities that go to the benefit of the individual. [See also comment under Definitions: Treatment] This is an excellent example of how computerization can assist caregivers in coordinating the best care for their patients – and this is on behalf of the individual, rather than on behalf of a patient population (fundamental difference with health plans).

Deceased Persons (Section 164.506(f))

Under the proposed rule, individually identifiable health information would continue to be protected for two years after the death of the individual, except for research purposes. For research purposes, the two-year protection would not apply and information would be immediately available. For any and all other purposes, covered entities would be able "to use such information or to disclose records to others, such as commercial collectors of information, two years after the death of the individual." (59951). **The AMA strongly**

**objects to the proposed regulation's construction and the Secretary's dismissive approach to protecting deceased persons' and their families' confidentiality.**

Traditional privacy law, which supports extinguishing an individual's right to control use or disclosure of information about oneself post-mortem, does not fit well with medical ethical obligations to keep patient confidences or the potential for misuse of personal medical information made possible by today's "Information Superhighway." The AMA believes that ethically little distinction can be made between protecting an individual's health information during life and protecting it post-mortem. Fostering open communication between patients and their physicians by protecting patient confidences during life as well as after it is sound policy for quality patient care. Fear of widespread and open disclosure of personal health information -- whether before or after death -- may cause patients to suppress information that is important for physicians and other health care practitioners to know in order to appropriately treat them.

Of course, confidentiality protections cannot be absolute. The AMA recognizes that several legitimate reasons for accessing deceased persons' health information exist. These reasons include fulfilling an individual need (for example, allowing limited familial access to genetic information) and addressing public health concerns (for example, initiating communicable disease contact tracing of a deceased persons' sex partners). Outside of this, we find only a few legitimate reasons why someone would need to review another individual's confidential health information post-mortem.

Commercial enterprises designed to access a deceased individual's private information are suspect. The AMA strongly opposes covered entities' commercial gain from disclosing individually identifiable health information, regardless of the passage of time after a patient's death. Therefore, unless sufficient oversight for commercial access is put in place, the AMA must strongly oppose the proposed regulation's provision of commercial access two-years after a patient's death. Such construction contravenes the spirit of AMA's Ethical Opinion 5.075, "Confidentiality: Disclosure of Records to Data Collection Companies," which warns physicians that it is violation of confidentiality to disclose information to commercial interests without authorization by patients.

**Though we oppose the proposed regulation's limited protection; if the Secretary chooses to keep the arbitrary two-year rule, we would support the Secretary's permission for "information holders [to] choose to keep information for a longer period" (59950). We recommend that this permissive language should be included explicitly in the regulation's language so that physicians may comply with their ethical obligations to patients.**

We offer the following comment with respect to the proposed regulation's note that "[w]e considered extending the two-year period for genetic and hereditary information, but were unable to construct criteria for protecting the possible privacy interests of living children without creating extensive burden for information holders and hampering health research" (59951). The AMA believes that genetic health information should be protected until the living children who may benefit from disclosure reach the age of

maturity, though it may be appropriate to disclose information sooner if benefit to the minor would outweigh the harm resulting from disclosure.

Research and similar activities for the benefit of public health or other specified public good, we believe, could be conducted using de-identified information or under the supervision of an IRB or similar body. **Therefore, in response to the Secretary's solicitation of comments in this regard, we offer that the proposed regulation's exception for research is unnecessary, and that existing research using deceased persons' individually identifiable health information could proceed under the requirements of proposed Section 164.510(j).**

We recognize that there will be many cases in which a legal representative's authorization would be difficult, if not impossible, to obtain. In these instances, we believe that the research involving deceased persons' individually identifiable health information, like other research, should be conducted under IRB (or similar body's) supervision. In this way, at least there would be some degree of assurance that all reasonable steps are taken to protect deceased persons' and their families' confidentiality. Such an approach would be consistent with the Secretary's recognition that "the privilege of using individually-identifiable health information for research purposes without individual authorization requires that the information be use and disclosed under strict conditions that safeguard individuals' confidentiality" (59967).

A particularly complex problem brought to our attention by the transplant community arises in the context of human tissue, fluids, eyes or organs that are donated for transplantation, but which prove unsuitable for this purpose. Generally, the transplant community will attempt to coordinate with the research community so that such donations can at least be used for research purposes. This would seem to be consistent with any altruistic intent of the donor or donor's family, and the rule should not present an obstacle to these transfers, particularly when time may be of the essence in preserving these materials.

Since the donor or donor's family must generally consent to any transplant purposes, it would seem to be a minimal additional obligation to seek consent for research purposes at the same time, should the material be unsuitable for transplant. Consent would obviate the need for additional IRB review for confidentiality purposes, since one would expect that the research project for which the human tissue or organs would be needed would have already received IRB approval. At the same time, IRB review would seem to be inconsistent with the ability to obtain and use such human materials.

In instances where evaluation for transplantation is *not* an element in the health information and human materials gathering process, we would expect an IRB review of research protocols regarding confidentiality of information to follow the requirements set out in Section 164.510(j).

<u>Components Entities</u>

**We approve of the proposed rule's construction whereby entities that provide health care, even if only in a discrete portion of the entity's conduct of business, should be treated as "covered entities" under the rule.** Examples might be school health clinics, on-site employee health services offered by businesses or, the problematic example, employers who operate self-funded health plans for their employees. Our key concern in these instances is in assuring that firewalls exist between the health provider function and all other elements of the entity. **We believe the proposed regulation should be modified to expressly recognize the necessity of such firewalls, particularly as the provision might relate to employer-sponsored health plans. Currently, while this intent is expressed in the preamble, its implementing language is not found in the language of the regulation itself.**

**While one draws the conclusion that employers who are self-funded *and* those with ERISA plans are covered entities under the definition of "health plan" (Section 160.103), clarifying language should be included elsewhere in the regulation to remove any ambiguity in construction and to make explicit that they be included in any such definition.**

**The AMA also recommends that Section 164.518(c)(3) be modified to make explicit that such firewalls must exist when a component entity that would qualify as a "covered entity" is part of a larger organization that would *not* qualify as a "covered entity."** Employees must have confidence that information garnered for health purposes will not be used inappropriately by their employer, even though their employers pays in whole or in part for their health care. It is absolutely essential that the proposed rule address this widespread fear among individuals and make a strong policy statement forbidding such practices.

**It would be helpful, as well, to include explanatory paragraphs in the preamble describing exactly what behaviors would be expected.** This should include, for example, a statement that the firewalls imposed by Section 164.518(c)(3) would preclude the flow of information between the health care component and the rest of an organization's employees or management, without reprisal to either the employee whose information is at issue or the employee refusing to comply with an improper request for disclosure.

**Individual Authorization. (Section 164.508)**

**The AMA strongly supports a requirement for an individual's authorization for most uses of his or her identifiable health information. Thus, we support not only the standard articulated in Section 164.508 for use and disclosure of protected information for any purpose outside the regulation, but would advocate for a similar requirement for many disclosures and uses for which the Secretary has removed such a requirement.**

**We also support the provision prohibiting covered entities from conditioning the provision of treatment or payment on the individual signing an authorization for**

**additional uses. The one exception to this prohibition would be in continuing to permit treatment provided as part of a clinical trial to be conditioned upon receiving an authorization. The AMA supports this exception. We also believe the provision could be tightened by adding a prohibition of financial incentives, such as premium discounts, that might be used to encourage patients to sign authorizations.**

We believe that variations in the required elements of an authorization, depending on whether the authorization is initiated by the individual or by the covered entity, could be confusing to administer. On its face, how could one distinguish what party initiated the authorization, except by inference from the elements contained in it? **Given the unitary model authorization offered in the proposed rule's appendix, it would seem less subject to error to simply require one authorization, with an additional section that would be filled out if the authorization is initiated by the covered entity.**

While the preamble notes that covered entities and their business partners would be bound by individual authorizations' limitations, we are unable to find an explicit provision in the regulation itself that reflects this intent. **Thus, we would recommend that a provision be added to Section 164.508 that expressly states that covered entities and their business partners must limit their disclosures and uses to the purpose(s) specified by the individual in the authorization.**

**It has been suggested by others, and we agree, that covered entities should be prohibited from seeking consent from patients for any marketing disclosures benefiting a third party.** The principle underlying this suggestion is that anyone who wants to obtain patient consent for marketing should be required to directly interact with the patient and not use a physician or other covered entity's relationship with the patient to suggest endorsement or approval. Such a prohibition would also decrease any incentive that covered entities might have to conduct business with such marketers.

**Lastly, we strongly object to the provision that would prohibit covered entities from seeking an authorization for treatment, payment or health care operations (Section 164.508(a)(2)(iv)), and recommend its removal.** This provision flies in the face of medical ethics and directly contradicts the Secretary's expressed intent in the preamble. The preamble notes that the "uses and disclosures that would be permitted under the proposed rule would be just that – permissible." When disclosures are not compelled by law, physicians would presumably be free to use their professional judgment as to whether to allow a disclosure. Indeed, the preamble continues, "[W]e propose these rules as a basic set of legal controls, but ethics and professional practice may dictate more guarded disclosure policies." (p. 59926) Yet the section at issue proposes to prohibit physicians "from seeking individual authorization for uses and disclosures for treatment, payment and health care operations unless required by State or other applicable law." We find the expressed intent of the proposed rule and its actual application to be incompatible, here, as in many instances.

**<u>Uses and disclosures permitted without individual authorization.(Section 164.510).</u>**

Public Health (Section 164.510(b)).

This proposed rule states: "[w]e propose to permit covered entities to disclose protected health information without individual authorization to public health authorities carrying out public health activities authorized by law, to non-governmental entities authorized by law to carry out public health activities, and to persons who may be at risk of contracting or spreading a disease." [p. 59955]

The AMA has a long history of supporting appropriate public health reporting by physicians in support of public health surveillance.[7]. The AMA recognizes that physicians have an obligation to be aware of and comply with laws that pertain to participation in public health surveillance programs, and that physicians can be reassured by the level of vigilance to patient confidentiality that is characteristic of the vast majority of public health departments. Moreover, AMA policy recognizes that disclosure of personally identifiable health information to public health physicians and departments is appropriate "for the purpose of addressing public health emergencies or to comply with laws regarding public health reporting for the purpose of disease surveillance."

However, AMA policy also unequivocally states that "when breaches of confidentiality are compelled for reasons of public health and safety, those breaches [must] be as narrow in scope and content as possible, must contain the least identifiable and sensitive information possible, and must be disclosed to the fewest possible to achieve the necessary end." Thus, while the AMA strongly supports a vigorous public health system, we nevertheless believe that certain boundaries are compelled by respect for individual privacy.

**Before personally identifiable health information is disclosed to public health authorities or their agents, or to persons at risk of contracting or spreading a disease, a harm-benefit analysis should be performed to ensure that the personally identifiable health information is in fact necessary.** Not every disease poses a risk of significant magnitude to a third party or the public health to warrant disclosure. **Moreover, de-identified data should be used whenever possible.**

The preservation of the patient-physician is paramount and is the underlying rationale for such safeguards. "Physicians in administrative and other non-clinical roles must put the needs of patients first. At least since the time of Hippocrates, physicians have cultivated the trust of their patients by placing patient welfare before all other concerns. The ethical obligations of physicians are not suspended when a physician assumes a position that does not directly involve patient care." Policy H-140.956 (AMA Policy Compendium)

Regarding epidemiologic research on public health and problems, the AMA recognizes the need to guard against unduly restrictive barriers to patient records that would impede or prevent access to data needed for public health research. However, such research should be guided by the same principles for, and safeguards on, privacy and

[7] AMA Policies H-10.982, H-10.984, H-20.941, H-20.963, H-30.967, H-60.956, H-85.970, H-440.938, H-440.968, H-515.969, H-440.995, H-515.971, E-5.057)

confidentiality that apply to all other medical research. These breaches in confidentiality for a public health purpose are no different from any other breach of a patient's confidentiality that benefits others beside the patient. Therefore, those breaches should be as narrow in scope and content as possible, should contain the least identifiable and sensitive information possible, and should be disclosed to the fewest possible to achieve the necessary end.

**Public health physicians and departments conducting research should adhere to the following procedures discussed above and repeated here for emphasis: where possible, valid consent should be obtained before personally identifiable health information is used for any purpose. However, in those situations where specific valid consent is not practical or possible, either (a) the information should have identifying information stripped from it or (b) an objective, publicly accountable entity must determine that patient consent is not required after weighing the risks and benefits of the proposed use. Re-identification of personal health information should only occur with patient consent or with the approval of an objective, publicly accountable entity. In the case of real or potential public health threats (e.g., outbreaks of communicable disease), practicing physicians must consult with their public health colleagues to treat diagnosed disease and engage in medically appropriate disease prevention.**

Health Oversight (Section 164.510(c)).

The AMA agrees generally that oversight activities are critical to support national priorities; however, we believe that a majority of these activities could be conducted in a manner that is less intrusive and more sensitive to the need to protect confidential patient information. **While the preamble acknowledges that certain oversight activities can be conducted without individually identifiable information (with either de-identified or aggregate information), there is no provision in the regulation to encourage such de-identification.**

The preamble recognizes some of the goals of public agencies' oversight activities in the health care system: "to monitor the fiscal and programmatic integrity of health programs and of government benefit programs; to ensure that payments or other benefits of these programs are being provided properly; to safeguard health care quality; to monitor the safety and efficacy of medical products; and to ensure compliance with statutes, regulations and other administrative requirements applicable to public programs and to health care delivery." (p. 559957)

**We recommend that if identifiable information is used, it should be accompanied by a limitation on further uses or access by other entities.** Our chief concern here is that access by health oversight agencies does not become a backdoor for law enforcement access. When does programmatic and fiscal oversight evolve into investigation? The line appears to be almost deliberately blurred between oversight activities and law enforcement activities and, in fact, the preamble states that "[a]gencies that conduct both oversight and law enforcement activities would be subject to this provision when

conducting oversight activities." (p. 59958) Yet the definition of "health oversight agency" includes many functions that overlap significantly with the definition of "law enforcement" and the activities described respectively.

The proposed rule does not offer any additional administrative or judicial process prior to disclosure for health oversight purposes that evolve into law enforcement actions. **At a minimum, the rule should contain a provision that precludes information garnered through health oversight activities to be used against the individual in any action unrelated to the oversight purpose.** People must be assured that the government is not engaged in "fishing expeditions," rummaging through intimate records without cause, looking for wrongdoers. Such unfettered access is reminiscent of law enforcement's warrantless search of homes in violation of the Fourth Amendment. As a matter of public policy, the Secretary should make it clear in this rule that such impermissible intrusions would not be tolerated.

Judicial and Administrative Proceedings (Section 164.510(d)).

Under this rule, disclosure would be permitted for purposes of judicial or administrative proceedings if the request is made pursuant to an order by a court or administrative tribunal. A court order would *not* be required if the protected health information requested related to a party to the proceeding whose health is placed at issue, or if the disclosure would be otherwise permitted under the proposed rule. **While the AMA supports the general provisions of this section, we recommend strengthening the language to increase objectivity and to limit subsequent unauthorized use and re-disclosure.**

An order by a court or administrative law judge provides some opportunity for an objective screening mechanism to balance the interests at stake in the proceeding. **We believe this objective screen should be uniformly imposed and object to the inclusion of a mere lawyer's letter – without benefit of a court order – as an acceptable "certification" that information is needed and relevant.**

The court order should establish that the information sought is necessary to the inquiry; that the needs of the requester cannot be satisfied by non-identifiable health information or by any other information; and that the need for the information outweighs the privacy interest of the individual to whom the information pertains. Subsequent uses and re-disclosures could be explicitly limited by adding a provision to the proposed rule that would require court or administrative orders to certify the following:

- the nature and scope of the information to be disclosed, with as much specificity and as narrowly tailored as possible;
- who is authorized to access such information (including a prohibition on subsequent disclosures to unauthorized individuals or entities); and
- that the information at issue is subject to court protection, including imposition of appropriate security measures.

In addition, the court or administrative panel should be empowered to impose any additional protections it believes is necessary to protect the confidentiality of information disclosed to it.

Further, the individual who is the subject of the record at issue must have an opportunity to know that his or her record has been requested for a judicial or administrative proceeding and should have the opportunity to object or limit the scope of the disclosure. **We recommend that the proposed rule include some notice requirement to the individual who is the subject of the record, concurrent with the request made of the record-holder for disclosure.**

Law Enforcement (Section 164.510(f))

The proposed rule permits disclosure of information without authorization from an individual if the request is made pursuant to a warrant, subpoena or order issued by a judicial officer. The AMA appreciates the Secretary's strengthening of these provisions from her original recommendations to the Congress in 1997. However, we believe that the proposed rule is still fundamentally lacking, in that it fails to require independent judicial review for *all* requests for disclosure of protected health information to law enforcement officers.

As long as the rule retains any kind of process whereby law enforcement can obtain medical records without objective judicial review, it encourages – even if unintentionally – law enforcement to use this process in order to avoid more protective requirements. **We recommend the deletion of the provision that would allow disclosure on the basis of an administrative subpoena or summons, civil investigative demand or any other instrument without independent judicial review.**

The AMA believes strongly that the requesting law enforcement entity should be allowed access to medical records only through a court order. Our position is that a strong legal standard, accompanied by a set of parameters on need and use, is essential to protecting not only personal medical information, but the confidence of citizens in their government.

This court order for disclosure should be granted only if the law enforcement entity has shown, by clear and convincing evidence, that (1) the information sought is necessary to a legitimate law enforcement inquiry; (2) that the needs of the law enforcement authority cannot be satisfied by non-identifiable health information or by any other information; and (3) that the law enforcement need for the information outweighs the privacy interest of the individual to whom the information pertains. The court order or administrative order should explicitly state

- the nature and scope of the information to be disclosed, with as much specificity and as narrowly tailored as possible;
- who is authorized to access such information (including a prohibition on subsequent disclosures to unauthorized individuals or entities); and

- that the information at issue is subject to court protection, including imposition of strict security measures.

In addition, the court or administrative panel should be empowered to impose any additional protections it believes is necessary to protect the confidentiality of information disclosed to it.

This is not an abstract concern. Physicians and their patients have repeatedly experienced the intrusion of law enforcement into patients' personal medical information when no need for identifiable information is established and no protections are provided. The unfortunate result is less – rather than greater – confidence in the law enforcement and judicial systems of this country.

Some government entities display the unfortunate tendency to consider patients' rights of confidentiality and privacy a luxury one may jettison randomly and without consequence. There is every possibility that such disregard for individual rights could increase under the proposed regulation in its current form, as it provides virtually unlimited access by investigators to medical records and fails to incorporate any protection for patients, even when patients are not the subjects of the investigation.

As the Secretary notes in the preamble, "if a misperception were to develop that law enforcement had instant and pervasive access to medical records, the goals of this proposed regulation could be undermined." (59961)

The AMA also has specific concerns regarding Section 164.510(f)(3), addressing "Information about a victim of crime or abuse," which we believe is too permissive. We believe that the provision does not adequately consider the needs and rights of the individual who is the victim of the crime. A breach of confidentiality of a victim's medical information has the potential to cause additional harm to the victim. Physicians face an uneasy quandary: for mentally competent adult victims of abuse, physicians are ethically obliged to not disclose an abuse diagnosis to spouses or other third parties without the consent of the patient.[8] Yet, physicians are also obliged to comply with reporting laws and, by doing so can help to set in motion further protection of the patient by law enforcement, social services and others. Generally, however, we support the principle of requiring a competent adult victim's consent before disclosing his or her identifiable information, and believe it should be adopted here. As the preamble suggests, many other sections of the proposed rule, as well as existing laws and even the consent of the victim, provide avenues to help identify those guilty of abusing or harming others; we should not create a mandatory disclosure requirement that has the potential of further victimizing crime victims.

<u>Governmental Health Data Systems. (Section 164.510(g))</u>

The AMA strongly objects to the troubling premise seemingly underlying the entire proposed rule, and particularly evident here, that government oversight of the efficiency

[8] AMA Ethical Opinion 2.02, "Abuse of Spouse, Children, Elderly Persons, and Others at Risk"

and effectiveness of the health care "system" is somehow a more compelling national priority than protecting individual citizens' right to privacy. We cannot agree with reasoning wherein the federal government appears to value even marginal increments of administrative efficiency over the basic rights of individuals to protect the privacy of their own health information.

The preamble to the proposed rule notes that governments "use information to analyze health care outcomes, quality, costs and patterns of utilization, effects of public policies, changes in the health care delivery system, and related trends**." The AMA sees no reason why these research and policy analysis purposes could not be fulfilled using de-identified individual or aggregate information. Further, if the government believes it requires individually identifiable health information for its particular purpose, it should be required to obtain the individual's consent for such disclosure and use, or to justify the value of the proposed project and the reasons why obtaining consent is impracticable or impossible. In these latter cases, an independent, publicly accountable balancing mechanism should be in place to evaluate the proposed need with the potential for harm to the individual and the security measures in place to preclude further dissemination of individuals' information.**

Amplifying this problem of government's apparent sense of entitlement to this information, the preemption provisions of the proposed regulation would permit the Secretary to impose the *lower* federal standard on a State that has created its own higher standard regarding the government's ability to access its citizen's most private medical information. This is the plain result of Section 160.203(a)(iv), which allows such Secretarial discretion "for purposes related to improving the Medicare program, the Medicaid program, *or the efficiency and effectiveness of the health care syste*m;" (emphasis added).

A recent example in the State of Wisconsin is instructive. In 1997, Wisconsin passed a data collection bill designed to collect individually identifiable patient information about every patient encounter, with the goal of being able to analyze and reduce healthcare costs and improve quality of care. Subsequently, the State Medical Society of Wisconsin undertook a public education campaign that revealed citizens' fears that, once in the hands of any governmental unit, there would be no way to guarantee that individuals' private health information would be safe from access by employers, marketers or others. The Wisconsin legislature heard resoundingly from their constituents one clear theme: patients do not want the State to have their private, confidential and identifiable medical information without their consent. The law was subsequently amended to prevent the State from obtaining identifiable information without consent.

Directory Information (Section 164.510(h))

The proposed rule would permit covered entities to disclose information for purposes of a facility directory if an individual consents to such disclosure. The preamble suggests that in the case of an individual who is incapacitated and who has not expressed a preference

in this regard, the covered entity could look to either a legally recognized surrogate or could decide itself, consistent with good medical practice.

**The AMA believes that the proposed rule addresses the chief concerns regarding availability of directory information and particularly commends the Secretary for recognizing the importance of consent in releasing even the most perfunctory information about an individual in a facility.** If the individual is unable to make his or her wishes known, a surrogate "steps into the shoes" of the patient to decide what may be in the patient's best interest. This is entirely consistent with the AMA's approach to consent for disclosures**.**

Banking and Payment Processes (Section 164.510(i)).

The proposed rule would allow covered entities to disclose protected health information to financial institutions, or entities acting for financial institutions, if necessary for processing payments for health care and health care premiums. Limiting the amount of information that financial institutions may receive to conduct the limited list of purposes set out in HIPAA is a good first step in controlling the flow of identifiable data. We also commend the prohibition against including any diagnostic or treatment information in data transmitted to financial institutions, as described in the preamble. It is not enough, however.

As stated previously, the AMA is very concerned with the limited jurisdiction of this proposed rule under HIPAA because it only applies to health care providers, health plans and health care clearinghouses. We recognize that financial institutions are not within the scope of this regulation, and that we must turn to Congress for meaningful restrictions on financial institutions' uses and re-disclosures of individually identifiable health information. The need for Congressional action is particularly imperative in the wake of the recent signing of the Financial Services Modernization Act, which removes the barriers that formerly precluded affiliated financial services entities from sharing information, including protected health information.

**The AMA believes that financial institutions should be subject to compliance with the provisions and the penalties for a knowing misuse of individually identifiable health information. Furthermore, individually identifiable health information and associated data should only be used to facilitate legitimate administrative and financial transactions as envisioned by the regulation and must not be used by either health plans, clearinghouses, other organizations or related commercial entities for marketing or other uses that could threaten the privacy of an individual or a physician.**

**We particularly object to the inclusion of bill collections among the functions permitted by entities acting on behalf of financial institutions, for which no privacy protections would attach. If the Secretary retains the "business partners" provisions of the rule, bill collection businesses should be considered "business**

**partners" under the proposed rule and subject to the contract provisions requiring confidentiality of protected health information.**

Research (Section 164.510(j)).

**The AMA strongly supports the extension of the Common Rule to all entities conducting human subject research, regardless of their federal nexus, and applauds the Secretary's efforts in this important area.** The weakness in this Section, as in much of the proposed rule, is the statutory limitation on the Secretary's authority under HIPAA to regulate researchers, unless those researchers are also acting as physicians or providers, as in a clinical trial. Thus, the provisions are targeted to physicians, providers and plans that use and disclose such information.

We believe that, as a general rule, an individual's consent should be obtained before personally identifiable health information is used for research purposes. We also recognize that it is not always possible or practical to obtain individual consent. In such cases, two alternatives are acceptable: the information should be de-identified, with safeguards in place to prevent re-identification by unauthorized individuals, or a waiver of consent must be obtained from an objective and publicly accountable oversight body, such as an Institutional Review Board (IRB).

The proposed rule generally fits these guidelines and permits covered entities to use and disclose protected health information for research without authorization, provided that the research has been reviewed by an Institutional Review Board (IRB) or equivalent body. The AMA is pleased that the Secretary has taken this approach and would like to suggest further refinements to the Research provisions of the proposed rule.

In the quarter century they have existed, IRBs have transformed the conduct of research involving human subjects. It is estimated that there are between 3,000 and 5,000 IRBs in the United States. Of these, approximately 1200 States are currently under public oversight; the reaming IRBs are private. While the majority of IRBs are associated with a hospital, university or other research institution, IRBs also exist in managed care organizations, government agencies, and independent for-profit entities contracting with organizations that conduct research.

Despite weaknesses that have been identified in recent years regarding their inability to keep up with their increasing workloads, IRBs have generally performed satisfactorily in protecting human research subjects. Confidentiality, however, is not a major focus of the Common Rule or IRB review. In recent testimony given to the U.S. Senate Committee on Health, Education, Labor and Pensions, the GAO concluded that "the process of IRB review does not ensure the confidentiality of medical records used in research – primarily because the provisions of the Common Rule related to confidentiality are limited."[9]

---

[9] "Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections is Limited," GAO/T-HEHS-99-70, February 24, 1999.

We are therefore pleased to note the proposed additions to the Common Rule that would better address the protection of individually identifiable information. We find the criteria in Section 164.510(j)(2)(iii), including standards from the Common Rule augmented by four additional standards, to be a reasonable approach to evaluating any research protocol. We do not believe these criteria are overly burdensome, nor do we expect that they will impede legitimate research. AMA policy recognizes that, while strong protections are necessary, they should not be so burdensome as to hinder important research or create unduly restrictive barriers for these legitimate activities. The burden under the Secretary's proposed rule, would weigh most heavily – as it should – on those researchers who cannot provide adequate privacy protections and who should not be provided access to sensitive information in the first place. Thus, the standard would prove to have served its purpose in screening out illegitimate or ill-conceived projects and in obliging researchers to protect their subjects' privacy.

**The AMA would suggest adding further qualifications that would need to be documented by an IRB or privacy board:**

- **that the health researcher has fully disclosed which of the protected health information to be collected or created would be linked to other protected health information, and that appropriate safeguards be employed to protect information against re-identification or subsequent unauthorized linkages; and**
- **that the health researcher has presented adequate assurances that none of the data containing protected health information will be given, loaned, sold, disseminated, or otherwise disclosed to other parties.**

We agree with the Secretary's conclusion that the nexus of federal funding is irrelevant in deciding the question of whether human research subjects should be protected. As a matter of public policy, individuals should be protected if they or their information are the subject of health-related research. The source of the funding should not result in different levels of protection.

The proposed rule seeks to correct the current lack of a clear requirement or mechanism for IRB scrutiny of research proposals that fall outside the scope of the Common Rule. Quality assurance and quality improvement projects, marketing initiatives, disease management programs, and accreditation processes are a few of the uses of personally identifiable health information that do not currently require IRB oversight. Moreover, some organizations use personally identifiable health information to conduct certain activities that they do *not* define as "research activities," and thus are not submitted for IRB review. Several managed care organizations, for example, have informed the GAO that they do not define records-based quality improvement activities as research, so these projects are not submitted for IRB review.

The Secretary's request for comments on how to distinguish between health care operations and research, particularly health services research, highlights this gray area. It is this very inability to capture the distinction that helps make the AMA's case why patient consent, or some method to substitute for patient consent when consent is

impossible or impracticable, should be the guiding rule for using any individually identifiable health information.

The diversity of proposed uses illustrates the inherent difficulty in addressing these evolving functions within any static legislative or regulatory definition. It also suggests the implausibility of reaching consensus on which functions are appropriate and which are not. Health care systems must be dynamic and flexible to compete in today's economy. It would be foolhardy to expect that the current list of uses for health information will remain static. The Secretary notes this when she states that "the health care industry is changing and that these categories [of "health care operations"], though broad, may need to be modified to reflect different conditions in the future." (P. 59934) Why not create a system that accepts this fact and builds in enough flexibility, while continuing to place patients' rights to control their information in a preeminent role.

The AMA believes the question should be re-framed and that it is unnecessary for a single federal law to create an immutable, one-size-fits-all scheme. **We recommend application of the controlling rule iterated previously: valid consent should be obtained before personally identifiable health information is used for any purpose. For those many functions or circumstances for which patient consent is not feasible, the information would either have to be de-identified to be used, or the decision regarding its use without patient consent would be made by an objective, publicly-accountable process that weighs the risks against the benefits of the proposed use.**

**The AMA believes that: research projects that fall outside the purview of an IRB process, *as well as operational uses of personally identifiable health information*, should be subject to review by privacy boards, as described by the Secretary, and should be held to the same standards that apply to Institutional Review Boards.**

Such an approach honors the rights of the individual and the primacy of patient consent, in a manner consistent with AMA policy. It also creates an incentive to de-identify health information at the earliest possible opportunity, which is also consistent with AMA policy. Finally, it recognizes the reality that many circumstances exist in which it is not practical or possible to seek patient consent, nor is "de-identification" a viable option. Instead of abdicating responsibility for patients at this point, it would require an accountable entity to act on behalf of patients to evaluate the need for identifiable information and to weigh the proposed patient protections against the potential risk to patients.

One cannot get patient consent every time for every use or disclosure, but that does not obviate the responsibility to represent patients' interests in some manner when deciding whether, and with what protections, personally identifiable health information will be shared. The approach is consistent with AMA policy that cautions against creating unduly restrictive barriers to patient information for legitimate uses and creates a mechanism for those seeking medical records to establish their legitimacy. In short, it creates accountability.

Many parties strongly argue that patient consent is either unnecessary for personally identifiable health information to be used for these functions, or that such consent should be a condition of plan enrollment or facility admission. However, AMA policy explicitly states that "[e]mployers and insurers should be barred from unconsented access to identifiable medical information" and that "[a] patient's ability to join or a physician's participation in an insurance plan should not be contingent on signing a broad and indefinite consent for release and disclosure."[10] We vigorously support the provision of the proposed rule that embraces this principle.

Those who argue against such a rule cite concern that obtaining such consent or, alternately, evaluating the disclosure and use for each category for which identifiable information is sought would be an insurmountable obstacle. However, the AMA has concluded that this argument is invalid. For most management or administrative functions for which a plan or provider would use personally identifiable health information, its evaluation of (1) the practicality of obtaining consent, (2) the feasibility of "de-identifying" information, and (3) the relative weight of risk versus benefit would be directed toward the use of a large number or category of records, not each individual patient record.

The National Committee for Quality Assurance (NCQA) has also proposed in its "Accreditation 2000: Draft Standards for Managed Care Organizations and Managed Behavioral Healthcare Organization" that "managed care organizations [designate] an internal committee to create and review confidentiality policies and to review practices regarding the collection, use, and disclosure of medical information."

Some organizations use personally identifiable health information for purposes outside the scope of the current Common Rule, but voluntarily apply similar standards to their decision-making about such uses. The AMA's Task Force of Privacy and Confidentiality heard persuasive, detailed testimony from a prominent multi-site health plan affiliated with one of the country's largest and most prestigious academic medical centers that currently employs just such a process. Operational and management functions of this plan are reviewed by an internal confidentiality committee, whose task it is to decide whether identifiable information is needed for the project or function and, if personally identifiable health information is required, to impose and enforce the guidelines by which it is obtained and used. Similarly, information received by the Task Force from a pharmaceutical research and manufacturing company described their internal patient protection review mechanisms that extend beyond Common Rule-enforced requirements. Their responsible officer is subject to corporate accountability and potential liability exposure for decisions that harm individuals.

On the other hand, our AMA Task Force also heard troubling testimony that some institutions and investigators avoid IRB review for outcomes studies or utilization review by calling these functions something other than research. Further, when the research questions are proprietary and are not intended to contribute to generalizable knowledge, the use of personally identifiable health information generally occurs outside of the

[10] AMA Policy H-315-983, "Patient Privacy and Confidentiality."

purview of human subjects protection mechanisms. Submitting all analyses that use personally identifiable health information to either an IRB or a similar body would replace the focus where it belongs, on the patient and the responsible use of his or her personal medical information.

The Privacy Board Concept: The AMA has developed a model similar to what the Secretary terms "privacy boards" in the proposed rule; we refer to our model as Confidentiality Assurance Boards (CABs). As we envision it, the CAB or privacy board as a body could exist either within or outside the entity seeking to use personally-identifiable health information. Some organizations may wish to create an oversight body to fill the explicit role of the board. Other organizations may already have Medical Records or Patient Privacy Committees to which they could delegate the purpose and functions of the CAB or privacy board. An IRB or CAB situated within an entity would have to demonstrate its objectivity through adherence to consensually derived standards (e.g., that a community member serve on the body).

Other entities may find the formation of an explicit, dedicated CAB or privacy board infeasible. For example, physicians in small group or solo practices may not have a significant use for personally identifiable health information outside the treatment and payment context or may have insufficient resources to create a formal, accountable oversight mechanism. In these situations, the small group or solo practitioners may wish to join with others to create a shared CAB or privacy board, perhaps under the auspices of the state or county medical societies. Another option might be to formally adopt and utilize standard policies that are developed nationally, locally, or by a health care delivery organization to which the practice belongs. Finally, small practices could naturally fall back on their existing responsibility to obtain patient consent for specific uses and disclosures of patient information that were not anticipated in the original treatment plan or payment context.

Confidentiality protections in a small community may require a different strategy than those required for a multi-state study with a massive enrollment. Placing responsibility with local review bodies, such as IRBs or privacy boards, allows flexibility to take into consideration special local concerns that affect decisions regarding how best to protect individuals' privacy.

A final benefit is that the approach builds on existing structures and mechanisms, without creating a new intrusive federal bureaucracy. Implementation may require a modest financial cost, and while the AMA is concerned about cumulative costs of implementing this proposed rule in its totality, we do not believe the cost of the privacy board policy is an insurmountable problem. Even more than the financial investment, establishment of a privacy board/CAB approach will require education, time, and institutional commitment. Institutions and physicians must recognize that the cost of not doing it right is not doing it at all.

The question of how to assure accountability and objectivity in the functioning of a privacy board or CAB requires careful evaluation. The suggestion of a new federal

bureaucracy to oversee these activities is cumbersome and undesirable. On the other hand, the Office for the Protection from Research Risks (OPRR), within the National Institutes of Health, does not currently have the capacity or resources to take on such an oversight function. Public access, audit requirements, and serious treatment of egregious offenses must be possible while avoiding the imposition of an intrusive federal regulatory superstructure. **While this is not the perfect solution, the AMA would recommend that the Secretary of HHS, in consultation with appropriate stakeholders (including the AMA), conduct a study after the final rule has been in effect for a year to review the efficacy of the recommended IRB-CAB approach.** Through this mechanism any discovered weaknesses or unanticipated problems could be addressed promptly and in a targeted fashion.

The proposed rule omits any requirement for the location or sponsorship of the IRB or privacy board. We remain somewhat uneasy as to how this omission might affect the objectivity of a privacy board situated within a corporate entity, making privacy decisions on behalf of that entity. We are reassured to some degree, however, by the board's membership requirements under the proposed rule that would prohibit review by members with a conflict of interest with respect to a particular research protocol and would include at least one person not affiliated with the institution doing the research. These elements create an expectation of both objectivity and accountability that is necessary for public confidence in health research.

**A parallel effort must be undertaken by HHS to address the deficits that have been identified in the current IRB system. The AMA would support an effort to train IRB chairs, co-chairs and members in privacy principles and practices. We also encourage medical schools, teaching institutions and other entities that conduct medical research to assure that their IRBs are afforded adequate personnel and other resources to accomplish their mission to safeguard the rights and welfare of human research subjects.**

Emergency Circumstances (Section 164.510(k))

**We support the proposed rule's Section 164.510(k), which "propose[s] to permit covered entities to use or disclose protected health information in emergencies, consistent with applicable law and standards of ethical conduct, based on a reasonable belief that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of any person or the public" [59971].** Here, it is permissible to disclose protected health information even if seeking authorization is not timely or possible. We are pleased to note the Secretary's reference to ethical standards in this provision and her specific reference to the AMA's Ethical Opinion on Confidentiality.

Next-of-kin (Section 164.510(l)).

**The proposed rule in this section requires providers to gain explicit consent from competent individuals before disclosing protected health information to next-of-kin**

**or other family members. This stance is consistent with AMA ethical opinions on genetic testing results, informed consent, and confidentiality in general.** We appreciate the Secretary's additional criteria that physicians' and providers' actions be "consistent with good professional health practice and ethics."

This recognition of physicians' professional and ethical standards in this and the previous Section of the proposed rule are important, and the AMA believes that these standards should likewise qualify many other provisions of the proposed rule. While imposition of rules and practices to protect patient confidentiality may be a new concept to some health plans and health data clearinghouses, physicians have been held to an oath for centuries to keep their patients' information confidential. Physicians' ethical obligations are generally reflected in State licensure laws, as well. We believe that the proposed rule should refer to the ethical parameters that Medicine has imposed on its own practitioners as a measure of physician compliance and not attempt to superimpose federal rules over physicians' existing ethical and legal obligations.

**Rights of individuals.**

The AMA supports the rights of individual to access their medical records, subject to limited exceptions, which is the approach adopted by the Secretary. We believe that the physical record and notes made in treating the patient belong to the physician; however, the information contained in the record is the patient's. Thus, certain rights should attach for both the patient and the physician.

The Secretary requests comments on whether health data clearinghouses should be subject to all the provisions of the Individual Rights section of the proposed rule. Aside from the responsibility to account for disclosures beyond those for purposes of treatment, payment of health care operations, the clearinghouses would be exempted from the rule's requirements, except as it might apply to them as "business partners" of a covered entity. We have commented elsewhere that it is confusing and unhelpful to permit covered entities to also characterize themselves as "business partners" under the rule; however, it may be unavoidable in this iteration of the rule. **At a minimum, clearinghouses should be required to establish notices of information practices to be made available upon request; and to accounting for disclosures upon request (as the proposed rule now would have them do).**

Notice of Information Practices. (164.512)

**We believe that health data clearinghouses should be, at a minimum, required to develop a written notice of information practices and make it available upon request.** While clearinghouses do not have the personal relationship with individuals that providers or even health plans do, they nevertheless use and disclose protected health information and have an obligation to the individual based on that activity.

The Secretary requests comments on the benefits and burdens of requiring a signed acknowledgement that an individual has received the physician's, provider's or plan's

written notice of information practices. We believe that a signed acknowledgement has several benefits. It alerts the patient that the notice they are signing contains important information and opens the door for discussion with a physician, provider or plan about its privacy practices. It may also be a good risk management practice for covered entities. However, the administrative burden of requiring such an acknowledgement must be considered, as well.

If a requirement for a signed acknowledgement is to be considered, we must also contrast it to the value of a proper consent form. The proposed rule's adoption of a patient's right to notice of the information practices of covered providers and plans will assist patients in understanding how their information will be used and disclosed. However, it does not provide patients the control over their information that is implied in the doctrine of confidentiality. AMA policy requires that confidentiality be protected and only allows the disclosure of information with a patient's authorization or when an objective analysis concludes that the benefits of disclosure outweigh risks to patients' privacy. The process of obtaining consent carries with it an expectation that a patient is informed of the practices of a provider or plan *and* provides the patient with a choice. A mere notification of the practices does not rise to this level of respecting the autonomy of the patient.

Furthermore, requiring patients to sign such a notification would give it the appearance of an agreement between the patient and the provider or plan. In fact, individuals would have no control over the terms of the practices. Therefore, while we believe notification is important, we do not believe it constitutes an adequate substitute to authorization to specific uses or disclosures. The administrative burden of requiring a signed notification does not seem to be significantly different from that which might result from requiring a signed consent.

The Secretary has requested comment on the level of detail that such a notice might be required to provide. The level of detail that to be included in describing uses and disclosures for health care operations should be adequate to alert the patient to the multiple categories for which their information is being used. Patients generally enter a physician's office or a hospital believing that the information they provide is going to their individual care and benefit. Activities that use individuals' information for the benefit of a population or group should be explained with some more specificity. This is particularly true since the accounting for disclosures provision would not include accounting for disclosures made for treatment, payment and health care operations. We would recommend against a uniform model notice, however, in that it could never capture the varying practices of covered entities and would not seem to be a significant improvement over today's blanket consent forms.

**We strongly oppose the suggestion that added notice format specifications, beyond those already provided in the proposed rule, might be required.** The Secretary repeatedly refers to the virtue of "scalability" in the proposed rule, to take into account the varying levels of sophistication of a physician's practice. We would urge her to

continue to demonstrate this restraint in not micro-managing the administrative affairs of a practice, including the formatting specifications of patient communications.

Access for Inspection and Copying (Section 164.514).

The AMA concurs with the Secretary's general approach allowing patient's access to their records, with very limited exceptions. The ability for patients to access their health records for inspection and copying enhances the openness and foundation of trust that characterizes the patient-physician relationship. AMA Policy explicitly states that "a patient should have access to the information in his or her health record, except for that information which, in the opinion of the health care professional, would cause harm to the patient or to other people."[11]

As noted previously, the new concept of "designated record set " has the potential to be quite confusing. What records would this involve? The proposed rule should not narrowly limit the character of protected health information one may access about one's self. However, we believe that most instances in which an individual is requesting access would be for a specific purpose that could be narrowed to ease the administrative burden of the covered entity and the confusion of large amounts of irrelevant information for the individual. In some instances, a summary of pertinent information may be more helpful for the patient's purpose than, say, a series of indecipherable billing codes, in which case the proposed rule should provide the authority for physicians to supply portions of a record or record summaries in lieu of a full copy of the records. Obviously, there are instances where this could be unacceptable, as in litigation discovery requests, so the rule should be permissive rather than obligatory.

Regarding individuals' access to records that may be stored off-site from the facility from which they are requested (for example, if the business partner holds custody of the records), we believe additional time may be needed for retrieval and recommend that the time limit be modified to permit an additional 30 days in these circumstances. The Secretary has requested comment as to whether a requirement for covered entities to acknowledge requests from individuals would be too burdensome. We believe that it would be too burdensome for smaller entities in particular and agree with the Secretary that covered entities may, but should not be required, to provide such acknowledgments.

We are pleased to note that the proposed rule would permit physicians and covered entities to charge a reasonable cost-based fee for copying health information provided pursuant to this Section. AMA's Code of Ethics permits such a reasonable fee and we believe it is a fair approach to bearing the cost for this service.

We approve of the permissive element attached to the grounds for denial, incorporating the exercise of reasonable professional judgment in deciding whether or not to deny access to all or a portion of a patient's record. We would recommend a change to Section 164.514(b)(i), so that situations in which a physician may deny access also include those

[11] AMA Policy H-140.989 "Informed Consent and Decision-Making in Health Care."

in which access might be reasonably likely to cause psychological or mental harm, as well as endangering the life or physical safety of an individual.

The exception in Section 164.514(b)(iv), regarding access to clinical trial records should be modified so that access can only be denied if the individual waives his or her right to access as part of the consent process and the clinical trial is in progress (currently in the proposed rule) *and* the patient's access to their individual information has the potential to compromise the integrity of the clinical trial. Given that some clinical trials last for years, and that many trial participants drop out, we believe there should be some way for participants to access their records in these cases, as long as their access does not destroy the integrity of the protocol.

Accounting of Disclosures (Section 164.515).

**The AMA supports the construction of the rule that would not require that "disclosure logs" be independently maintained, but that would require a covered entity to be able to provide an accounting of disclosures upon request of an individual.** It is important that individuals know where their medical information is going; however, this must be balanced with the potential administrative burden of requiring an accounting of all disclosures when it is anticipated that relatively few individuals will seek such accounting. We believe the Secretary has generally struck this balance successfully.

The Secretary solicits comments on whether a specific limit should be put on how far back in time that the covered entity must be able to account for disclosures. The proposed rule would require that covered entities be able to account for disclosures as long as the entity maintains the record. While some federal and State laws require record retention for a specific number of years, others remain silent on the subject, preferring an implicit public policy for record retention that conforms to liability laws and statutes of limitation. **The language of the proposed rule that refers to the length of time the entity retains the record itself could be clarified to state that whatever minimum requirements are in place for the record should also guide covered entities in retaining their capacity to account for disclosures over that same time, but no longer.**

For disclosures that the individual authorizes in writing, we are perplexed as to why the individual would not have some responsibility for maintaining a file of his or her own authorizations. **While these disclosures may also be part of the covered entity's record, we believe they should be an optional element of the entity's accounting for disclosures, rather than a required element.** Of course, the burden in including this category of disclosures may not significantly increase the overall burden of a covered entity in providing the accounting, and it may include such disclosures; however, it should not be required.

Amendment and Correction. (Section 164.516)

While we recognize that individuals should have the right to request that erroneous information be corrected in their medical records, the AMA believes that this right must accommodate the need for clinically and legally accurate records. For example, we object to the proposed rule employing the terms "amendment and correction," as patients are likely to understand these words in their vernacular sense to believe that they may *change* their medical records. This expectation will only sow discord between patients and their physicians and permit the medical record to become a forum for disputes**. We think it is less misleading and more technically correct to refer to the right to "append" information to their record.**

Physicians may not obliterate or change the medical record; they may make additional notations explaining mistakes, but are under a legal obligation to maintain a record that reflects what was thought to be correct at the time a notation is entered. **We also believe it is extremely important for the proposed rule to reflect explicitly that patients are *not* authorized by this section to request changes in professional clinical judgments or treatment recommendations that they believe to be in error. Neither should individuals be able to amend/append a clinical record by adding information about the type, duration or quality of treatment that individual believes he or she should have been provided.**

We also note that the proposed rule would allow a covered entity to refuse to correct a record it had not created. We have some concerns about the practical implications of such a provision. **If a covered entity is using misinformation in its decision-making, it should be authorized – though not required -- to correct the information at the request of the individual.** Although the AMA supports the concept that the originating physician should be alerted to the suspected error, we do not believe that that physician should necessarily be the gatekeeper for all record corrections, particularly those which go to non-medical information. It is up to the individual to identify those additional parties who should be notified of any material changes in the record that result from an individual using this provision.

**Administrative Requirements (Section 164.518)**

This provision sets out an extensive series of administrative requirements that physicians and other covered entities would have to incorporate into their practice or business. The AMA has significant concerns about the substantial administrative and financial burdens this might place on physician practices, particularly those smaller practices whose administrative personnel are already stretched to the limit with a multitude of governmental and health plan requirements.

It would require providers to designate a privacy official, train member of their workforce regarding privacy requirements, safeguard protected health information, and establish sanctions for members of the workforce who do not abide by the entity's privacy policies and procedures. Further, physicians and providers would be required to establish a means for individuals to complain to the covered plan or provider if they believe that their privacy rights have been violated. Training could include videos, and interactive

software. Trainees would have to be re-certified every three years. Retraining would be required if there were material changes in privacy policies or procedures. Safeguards would have to be established against "reasonably anticipated" threats or hazards. The identity and legal authority of persons requesting disclosure of health information would have to be determined. Some mechanism for receiving complaints would have to be established. Covered entities would be required to develop sanctions for failure to comply with policies or procedures. All members of the physician's or provider's workforce, as well as those of business partners, would be subject to the sanctions

**The AMA believes that the patient protections intended by such requirements are largely in place in most physicians' offices and strongly recommends that the flexibility/scalability in administration explicitly promoted by the Secretary be particularly applied in these instances.** These provisions highlight, yet again, the distinction that separates physicians from other entities covered under this proposed rule. Physicians' existing legal and ethical obligations require that they handle patient information confidentially, and these obligations are enforced through State law and State medical licensing boards. The addition of a federal superstructure of rules and regulations to achieve the same end is largely redundant and confusing. Health plans and health data clearinghouses have no such universal obligations, and so a new federal structure of regulations may be more appropriately imposed without disrupting current practice. **We urge the Secretary to accommodate physicians' existing procedures and obligations to the extent possible in enforcing the administrative requirements under this proposed rule.**

Privacy Official (Section 164.518(a)(1))

In our evaluation of the relative benefit and burden of this provision, we place special emphasis on the Secretary's commentary that the "implementation of this requirement would depend on the size of the entity." (p. 59988) While we acknowledge that it makes sense to designate one person, committee or office within an entity as the central focus for privacy concerns, we recognize that many small physician practices have limited or part-time staff who are already consumed with paperwork resulting from a flood of regulatory requirements**. It may be the case that several people share the responsibilities, and we do not see that this would impede the implementation of standards or the rights of individuals in any way. Thus, we would request a provision permitting such an arrangement for small physician offices**.

**We also suggest that there is room for clarification as to whether the appointment of a new privacy contact person in a physician's office would be considered a material change in the written notice of information practices. We suggest that it is *not* a material change, since the individual contacting the covered entity can easily be directed to the new person in charge of privacy for the office.**

Training (Section 164.518(b))

Again, we appreciate the Secretary's commitment to providing flexibility in application of the training standard that recognizes the varying needs of different sized entities. **We question the need for re-certification once every three years, and suggest retraining is necessary only if there is a substantial change in policy.** Employees could be reminded of their obligations in a less burdensome way, e.g., employee newsletters, notices posted in the workplace, staff rooms, or meetings. The signing of statements by employees (including all volunteers) that they will honor the workplace's privacy policies is marginally valuable as a risk management tool; rather, it may have greater value as a way to personally vest each employee with a sense of responsibility for keeping patients' records private.

Safeguards (Section 164.518(c).

In response to the NPRM first published in August of 1998, regarding "Security and Electronic Signature Standards," the AMA sent a strong letter requesting the withdrawal of the proposed rule, concluding that it "[flew] in the face of its intended goal of 'administrative simplification.'" We noted that, while the AMA supported physicians' transitioning to an electronic data interchange (EDI) environment, we believed the "proposed rule on security standards would impose such an excessive level of micro-management as to discourage physicians' offices from just such a desired transition." We are therefore troubled to note the Secretary's statement in the preamble that "we are proposing parallel and consistent requirements for safeguarding the privacy of protected health information."

The AMA supports the proposed rule's provisions that would not require painstaking verification of the identity or legal authority of individuals requesting protected health information under the rule. We appreciate the general, common sense principles articulated in the preamble. It is a little more difficult to verify the truthfulness of individuals presenting themselves as next-of-kin, however, and we would anticipate that reasonable attempts to verify identity would be adequate to establish a good faith defense if information was mistakenly provided to someone misrepresenting himself or herself.

Regarding the provision on "whistleblowers," while we appreciate the proposed rule absolving the covered entity of blame if an employee discloses protected health information to law enforcement, a health oversight agency or an attorney, we nevertheless must object to this provision. It would permit a single individual to substitute his or her judgment, perhaps impaired by malicious intent, to disclose protected health records. In some cases, it could be no more than a private sector "fishing expedition." We believe that "whistleblowing" employees, who have access to privileged and protected information as a function of their employment, should only be able to report suspected violations to law enforcement or health oversight agencies using de-identified or aggregate data. At the very minimum, a "minimum necessary disclosure" requirement should be imposed on such individuals to protect the privacy of patients who may be completely uninvolved in the suspected illegal activity that the whistleblower seeks to bring to law enforcement's attention.

Internal complaint process (Section 164.518(d))

We agree with the Secretary's assessment that imposition of a less intimidating complaint system will be more likely to encourage patients to discuss their concerns with their physician and we hope that it would preclude the necessity of filing a complaint with the Secretary. Given the continuing relationship that most patients have with their physician, it is important for conflicts to be resolved in a manner that encourages trust and cooperation between the parties.

Sanctions (Section 164.518(e)).

We believe it is adequate for physicians to evaluate violations by their employees and business partners as they occur and assess the most appropriate sanction. **The Secretary was unable in the proposed regulation to forecast each possible situation and its circumstances, and covered entities should not be required to do so either.** It should be enough for the proposed rule to encourage covered entities to impose sanctions.

Duty to mitigate (Section 164.518(f)).

Similarly, under the duty to mitigate, imposing the affirmative obligation to try to mitigate any deleterious effect of unauthorized disclosures or uses of protected health information by employees should be adequate. A prescribed mitigation policy could hardly anticipate ahead of time the unique circumstances to each violation for which mitigation might be required. **Thus, we believe it is adequate to create the obligation, to the extent practicable, for mitigation for employees' breaches.**

**In contrast, we do not believe a similar obligation is appropriate in the context of the business partners relationship.** Employees are at least nominally under the control of the employer covered entity, and so a duty to mitigate might be expected. Business partners are independent entities under contract with the covered entity and the covered entity should have no responsibility whatsoever under the proposed rule to mitigate damages resulting from business partners' prohibited acts. **This provision should be eliminated from the proposed rule.**

**Development and documentation of policies and procedures.**

Under the proposed rule physicians would be required to develop policies and procedures for implementing the provisions of the rule. The Secretary assures that, under the principle of scalability, the complexity and scale of the policies could be consistent with the size of the practice. Professional associations, such as the AMA, are urged to develop model policies, procedures, and documentation for their members.

In an ironic development, given the origins of the proposed rule in the "Administrative Simplification" provisions of HIPAA, the Secretary recognizes that this requirement "would impose some paperwork burden." This is an understatement of the investment in time, personnel and money that would be required to comply under the current proposal.

Not only would physicians be required to create, maintain, update and make available for audit a vast array of new documentation, they would be required to keep this newly imposed "library" on a rolling schedule of six years.

The AMA objects in the strongest terms to the school of bureaucratic thought that requires documentation that one is going to do something, documentation that one is doing that same thing, and documentation that the same thing has been done. Physicians and their office staffs are absolutely overwhelmed by current paperwork requirements generated by well-intended, but poorly thought out, regulations. Such redundant documentation requirements are for the administrative ease of compliance officers – not for physicians and certainly not for patients. Masses of documentation allow compliance officers to push their familiar paper and quibble over parenthetical clauses rather than to really investigate to see when a true wrong has been committed.

If the Secretary is concerned that an entity has not designated a privacy officer, what precludes the investigator from calling the physician's office and asking to speak to the privacy officer? Or requesting a notice of information practices that would contain the officer's name? Or any other inquiry sparked by complaints or concerns? Large and medium sized entities are more likely to have documented policies on every conceivable aspect of their operation as a function of their size and their risk management and legal departments. Smaller physician practices rely on less bureaucratic methods of communicating with their employees and their practice is incompatible with the enormous documentation burden imposed by this proposed rule. **The AMA recommends that the paperwork and documentation elements of the proposed rule be withdrawn completely and rethought with a more realistic and flexible implementation approach for smaller physician offices.** After all, is the goal to actually protect patient privacy, or is it to create paper saying that we do?

**Relationship to State laws**

AMA policy supports a preemption provision that preserves more stringent state confidentiality laws, so that federal and state privacy protections would be cumulative. Both the Congress, in HIPAA, and the Secretary, in her Recommendations to Congress and in the preamble to this proposed rule, have expressed a clear intent to allow more stringent state laws to remain in force under the federal regulation. We are deeply concerned, then, that while the proposed rule suggests that its preemption provision sets such a federal "floor," rather than "ceiling," a raft of subsequent exceptions and qualifiers completely undermine the provision.

The proposal generally would preempt those state medical record privacy laws that are "contrary to" the federal regulation, with several exceptions where the Secretary determines that the state law is necessary to:

- prevent fraud and abuse;
- ensure appropriate state regulation of insurance and health plans[this would include the reporting and access to records for the regulation of health plans, for

purposes of management and financial audits, program monitoring and evaluation, and individual or facility licensure or certification];
- for state reporting on health care delivery or costs;
- for state laws addressing controlled substances; and
- "for other purposes related to improving the Medicare program, the Medicaid program, *or the efficiency and effectiveness of the health care system*." (emphasis added)

In addition, state authority over public health reporting of disease or injury, child abuse, birth or death, public health surveillance or public health investigation or intervention would be preserved without any federal interference. Thus, *less protective* state laws intended to achieve any of the above purposes would prevail over federally imposed protections.

This provision duplicates, with one interesting twist, the statutory language of HIPAA (Section 262(a), "Section 1178(2)). The language of the last bullet qualifying "other purposes" as those "related to improving the Medicare program, the Medicaid program, or the efficiency and effectiveness of the health care system" derive from Section 261 of HIPAA, establishing the Purpose of Subtitle F, "Administrative Simplification." "Efficiency and effectiveness" are vague catch-all terms that would seem to confer broad authority for the Secretary to intervene for almost any reason. While the Secretary may have intended this qualifying language to narrow the scope of her advisory opinion authority, in fact, it tends to reinforce the fear that individuals repeatedly express: that governmental expediency will overrun their rights as citizens.

At the same time, "more stringent" state law regarding the privacy of individually identifiable health information would remain in force. However, the following qualifications and exceptions reduce this provision's applicability in all but a few cases.

- Administrative determinations as to whether a state law were "more stringent" than the federal requirement would be made by the Secretary, *upon request of a State*. Those entities – specifically physicians – regulated by the rule would not be able to independently query the Secretary for a determination; it must go through the State. Two implementation problems are immediately evident:

    - Physicians who seek to comply with state law, believing in good faith that it is more stringent than the federal standard, could be in violation of the regulation without ever knowing or having an opportunity to directly request guidance from the Secretary. We do not believe that HHS will be "inundated" with requests for clarification, in that the Secretary need only rule once on any request for exemption for it to apply to all entities in a State.

    - A State government could have a conflict of interest in bringing forward queries to the Secretary. States are frequently among the largest health data collectors, and it is not unthinkable that a State's executive branch might consider its "gatekeeper" function as an opportunity to keep the "gate" closed

to more protective State privacy statutes prevailing over less protective federal standards.

- Such determinations would apply *only to transactions that are wholly intrastate*. Thus, any element of a health care transaction that would implicate more than one state's laws would automatically preclude the Secretary's evaluation as to whether the laws were more or less stringent than the federal requirement. Given the interstate character of most health care transactions in which information flows from a physician to a hospital system or a plan, even the Secretary admits that "positive determination could be minimal under this provision."

- The Secretary would also be authorized under the rule to provide similar "guidance" by way of Advisory Opinions, again available only to the States' requests for evaluation. Patients and their physicians could not independently request an Advisory Opinion.

It is clear to the AMA that, read together, the exceptions to the preemption provisions of the proposed rule completely undermine the alleged intent of the Secretary to preserve "more stringent State laws." **The AMA continues to support our policy calling for any federal law or regulation regarding medical record privacy to provide a true "floor," rather than "ceiling," for patient protections.**

**Relationship to other federal laws.**

The proposed regulation's affect on other federal laws, considering how courts' resolve conflicts between two federal statutes, would appear to leave in place more specific or stringent federal law, such as the Substance Abuse Confidentiality regulations. Due to the proposed regulation's inadequate protection of patient confidentiality, generally we support this result.

The AMA, however, is concerned that the proposed regulation in its current form will confuse, rather than clarify, physicians' and other health care practitioners' obligations under federal law on patient confidentiality. To illustrate, under the Substance Abuse Confidentiality regulations, generally physicians cannot disclose information about patients' treatment for drug abuse to law enforcement officials; yet, under the proposed regulation, such disclosure is allowed without individual authorization. Seemingly, physicians and other health care practitioners will find themselves in a "catch-22," trying both to protect patient confidentiality under more restrictive federal law and accommodating requesters of information operating under the proposed regulation's permissive approach to disclosure of confidential patient information.

**Again, we recommend that the Secretary revise the proposed regulation to include more stringent protections for patient confidentiality.** In this way, potential conflicts among federal laws on confidentiality will be minimized.

**Compliance and Enforcement. (Section 164.522)**

We are encouraged to note the Secretary's philosophy of providing "a cooperative approach to obtaining compliance," that looks to an educational, rather than punitive, approach to resolve disputes. The AMA nevertheless questions the role of the Secretary or any federal officer to investigate complaints against physicians for breaches of patient confidentiality. This is the traditional realm of state medical licensing boards and their premier role in pursuing this type of activity is clearly articulated in state medical practice acts. As we have articulated throughout our comment to the proposed rule, physicians are *not* in the same category as the other entities covered under this proposed rule. Physicians are unique in that they have *existing* legal and ethical obligations to protect patients' confidentiality. Hospitals do not have this dual obligation. Health plans and health data clearinghouses most certainly do not have this dual obligation. And so it is understandable that the AMA's membership is perplexed at the prospect of a new federal regulatory scheme superimposed upon an existing set of obligations to accomplish the same goal. It is confusing. It is redundant. And it lumps physicians together with entities completely removed from a context of ethical and fiduciary relationships with patients.

In noting individuals' ability to file complaints with the Secretary for covered entities' alleged violations, we find it incongruous that covered entities cannot petition the Secretary for guidance in finding out what activities may be violations up front when the issue of State preemption arises. We are not, of course, suggesting that individuals not be able to petition the Secretary. Rather, we anticipate the frustration of physicians who will be seeking, in good faith, to comply with the rule and who will be unable to obtain a ruling as to how they might proceed in the face of conflicts with State laws. This is a significant failing of the proposed rule, in that physicians are regulated already by States and their activities, more than any other entity, will be subject to competing interpretations for compliance. (See also, discussion on Relationship with State Laws.)

The Department, under the proposed rule, is authorized to administer unlimited site reviews. **In the absence of specific complaints or allegations of wrongdoing on the part of physicians' offices, compliance reviews should be explicitly limited.**

Although the proposed rule does not specify which office in the Department would be responsible for compliance, the AMA is concerned about informal comments indicating that the HHS Office for Civil Rights may be designated. Our understanding of the rationale behind this choice is that this Office has experience in pursuing individuals' claims involving civil rights violations that would translate to the individuals' claims that would be made under the proposed rule. We believe that the first requirement of a compliance and enforcement office should be an understanding of the complexities of patient care and information handling within a physician's office or health care facility. This is particularly true if the Secretary's intention truly is to provide educational, rather than punitive, assistance. Only individuals who understand how medical records are used for patient care in innumerable settings will be able to offer the very flexibility and scalability in compliance oversight and enforcement that the Secretary pledges is her intent. If the Secretary is intent on such a delegation, we would urge her to provide the

necessary support and resources to offer just such expertise to complement the existing Office for Civil Rights.

**Small Business Assistance**

This section mentions a few features that are supposed to make compliance easier for small businesses, which are defined as businesses with less than $5 million annual revenue. These include assurances that written authorization for disclosure would not be required for "routine" uses of information (i.e., uses for treatment, payment, health care operations, or when required by law); that the Department of HHS would do outreach and education; and that HHS would collaborate with professional associations to create model forms and other tools to assist compliance.

We note that the preamble would provide "small businesses" an extra year, beyond the general two year deadline after final publication, for compliance. The Secretary cites several examples of small physician offices receiving "small business" assistance, and one would assume from reading the preamble that the extra year extension would apply to small physician offices. However, Section 164.524 of the proposed rule specifically cites "small health plan[s]" *only* as being eligible for this extension. **We urge the Secretary to include "small providers" or "small physician offices" in the actual regulatory language allowing 36 months for compliance, to fulfill her intent expressed in the preamble.**

**Preliminary Regulatory Impact Analysis**

The Department of HHS finds that this proposed rule is a "major rule" because it is likely to have an impact on the economy in excess of $1 billion in the first year alone. It is also found that rule is a "significant regulatory action," requiring congressional review. It is assumed that the greatest benefit will be increased patient trust and that privacy is a "right" that cannot be valued solely by market costs. The Department is "confident that future benefits will be higher than those stated in this analysis."

**Relationship of this Analysis to Analyses in Other HIPAA Regulations.**

The proposed rule notes that the "original HIPAA analyses did not incorporate the expected costs and benefits of privacy regulation because, at the time of the original analyses, we did not know whether Congress would enact legislation or whether privacy would need to be addressed by regulation. Therefore, much of our cost analysis is based on the expected incremental costs above those related to other HIPAA regulations."

The AMA stated in previous comments on HIPAA NPRMs that the stated burden estimates appeared to be very inaccurate. In addition, the Five-Year Net Savings as listed in the transaction proposed rule indicates that health plans will have much more to gain from electronic transactions than providers. Therefore, the health plans should take on the majority of the burden of the implementation costs.

In addition, based on the figures stated in the HIPAA National Provider Identifier (NPI) NPRM, the AMA believes that the costs of developing and maintaining the NPI need to be borne by the health plans that stand to reap a profit from the use of the NPI. We recognize the savings for practitioners are projected after the initial 5-year period. Nonetheless, health care practitioners should not be required to bear further costs under a system that already predicts that they suffer an initial monetary loss.

Furthermore, the AMA believes that the transaction and NPI cost estimates need to be recalculated using more current figures and to reflect current trends. Many of the figures for which these costs and savings were calculated were outdated, including the dates of implementation. Also, the AMA believes that the costs originally calculated for physicians are based upon a physician population of 404,000. However, based on the results published in the AMA's *Physician Characteristics and Distribution in the US 1999*, there are currently over 620,000 physicians in direct patient care with approximately 22,000 physicians being added to the population each year.

The AMA notes that the cost to comply with the proposed privacy regulations clearly is not a one- time cost but will be a perpetual and continuing commitment, and this should be reflected in the analysis. These continuing costs are not anticipated by the proposed rule. Furthermore, the proposed rule could impose significant new costs on physicians' practices. We believe this runs counter to the explicit intent of HIPAA's "Administrative Simplification" provisions, which require "any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care." (Sec. 262. "Administrative Simplification," "Sec. 1172(b) Reduction of Costs.")

**Summary of Costs and Benefits.**

Cost estimation is "difficult." There are very few data. Some requirements of the proposed rule are not estimated, which HHS recognizes "may be significant in some cases." Benefits are regarded as primarily a "right" and are therefore "difficult to measure."

The proposed rule asserts the following chain of causation: increased privacy of health information creates more confidence in health care among the public, which leads to more treatment being sought, which promotes improved health and ultimately reduced health care spending. But this line of reasoning is incomplete because it ignores the cost of the new treatments engendered by increased "confidence," so it remains an open question as to whether improved privacy really lowers health care costs in the long run.

The entire cost-benefit comparison seems to rest on a questionable assumption: "…if individuals would be willing to pay more than $0.46 per health care encounter to improve health information privacy, the benefits of the proposed regulation would outweigh the cost." Notwithstanding the accuracy of the cost estimate, this assumption weakens the entire quantitative economic justification for the proposed rule.

**Baseline Privacy Protections.**

Professional Codes of Conduct and the Protection of Health Information.

It is suggested that "the proposed rule embodies all the major principles expressed in the standards." At the same time, it is acknowledged that "there are some major areas of difference between the proposed rule and the professional standards reviewed." The comments offered by the AMA point to a conceptualization of confidentiality espoused by the proposed rule that does not provide individual patients control over their health information, a central element of the guidelines included in the AMA's Code of Medical Ethics. As an association of physicians dedicated to enhancing the patient-physician relationship, AMA policy considers patient autonomy to be a fundamental element of medical ethics that receives little attention in the proposed rule. The rights given to patients under the proposed rule do not given patients control over the use or disclosure of the protected health information. Yet, ethical reasoning requires confidentiality of health information to be protected by limiting the use and disclosure of information to instances where the patient gives his or her authorization, presumably having considered the advantages and disadvantages. Therefore, the AMA is concerned that the spirit of the proposed rule contravenes fundamental guidelines given to the medical profession in the Code of Medical Ethics.

**Costs.**

Estimated that compliance costs will total to $3.8 billion over five years, with a range of $1.8-6.3 billion. But, as already mentioned, this estimates excludes many provisions of the proposed rule that "may be significant." The elements that are estimated may be suspect as well.

Privacy Policies and Procedures. The proposed rule anticipates that few providers will develop their own procedures, relying instead on their "national and state associations." But it is not apparent that costs to those associations are included in the analysis. The cost per provider is estimated to fall in the $300-3000 range, with a weighted average of $375. But no justification is provided for these estimates, which seem very low.

System Compliance Costs. The estimated costs are based on two assumptions regarding percentages (i.e., 15% and 10%), but no justification is presented for the percentages chosen.

Notice of Privacy Policies. The first paragraph is concerned with how many notices would have to be provided annually. "Each entity will have a notice cost associated with each person to whom they provide services." That is, the first encounter between a patient and a provider should generate the issuance of a privacy notice; subsequent encounters between the same patient and the same provider would not matter. The language in the first paragraph uses survey data on "encounters," "patients," and "episodes" per year to estimate a total. These are different concepts, however, so the reported total of 397 million (corrected by HCFA from 350 million) is meaningless and it unclear what the

estimate represents. Further, no information is provided on how many potential patients there are, so the estimate of 543 million patients (encounters?) seen at least once over five years cannot be verified.

No evidence is presented to support the cost estimates for notice development and dissemination. A five-year cost of approximately $209 million for providers is presented. But it is not shown how this breaks down on an encounter basis. The estimate to plans of $0.75 per insured person seems very low. That might pay for postage but seems insufficient to cover labor and capital usage costs.

Inspection and Copying. It is assumed that 1.5% of patients will request access to inspect and copy their medical record. No justification is provided for this estimate. Being a small number, it would be easy for the estimate to be low. For example, if 3% (i.e., just 1.5 percentage points higher than the estimate) of patients made such requests, the cost estimate would double. The figure of 543 million unduplicated patient-provider encounters is used, which raises again the question of exactly what this number represents.

Amendment/Correction. Again, the cost estimate depends on two estimates: (1) the percentage of patients who request inspection and copying that also request amendment and correction (67%) and (2) the cost of making corrections ($75 per request). We have no way of knowing how accurate these estimates are, which weakens the analysis.

Authorizations. An assumption is made that 1% of encounters will require obtaining authorizations from patients before health information may be released to payers and other third parties. Providers will have to develop new procedures to conform to the proposed rule. There appears to be some confusion is the estimation of one and five-year costs. Total unduplicated patient-provider encounters over *five* years were previously estimated to be 543 million (p. 60016). One percent of 543 million is 5.43 million. At a cost of $10 each, the aggregate cost would be about $54 million over *five* years. The text on p. 60017 misinterprets this as "annually" and goes on to multiply this by five to get the stated five-year cost of $271 million.

Training. The assumed on-going cost of $20 per provider office per year seems absurdly low.

Conclusion. It is acknowledged once again that "the estimates do not consider all of the costs imposed by the regulation." We cannot overstate the onerous result of the cumulative effect each of these requirements for physicians, added to the already swollen administrative burden with which physicians must currently comply.

**Benefits.**

No attempt is made to estimate aggregate benefits directly. The proposed rule offers the justification that privacy protection is a personal right, which somehow makes it impossible to estimate benefits based on the market value of health information. An

alternative approach taken is to use *de minimus* cost estimates as hurdles to be cleared and then essentially argue that benefits certainly exceed that low barrier. This is argument by handwaving and is an attempt to divert attention from the fact that no real cost-benefit comparison is presented.

Compliance costs are presented as $3.41 per insured individual per year ($750 million per year divided by 220 million insured individuals). It is suggested that this is an upper-bound figure, because it spreads the aggregate cost only over insured persons and ignores the uninsured. However, adding in 44 million uninsureds and redoing the calculation reveals that the per-person per-year cost is $2.84, a difference of only $0.57. Yet another approach expresses compliance costs on a per-encounter per-year basis, which the proposed rule states as $0.46. It has been previously and repeatedly argued in these comments that aggregate cost estimates are too low, perhaps by orders of magnitude. ut none of these cost estimates is relevant in a discussion that is supposed to be about benefits.

The proposed rule discusses several examples of areas where increased confidence in privacy would have significant benefits. These comments will be restricted to one example: substance abuse and mental health treatment. It is alleged in the proposed rule that the economic cost of mental health disorders is approximately $115 billion per year. How this is divided between lost economic output and direct costs of treatment is not mentioned. It is stated that appropriate treatment could result in "hundreds of millions in cost savings annually," but it is not clear whether this includes the cost of the treatment. In attempting to connect improved confidentiality with economic benefits, the rule can do no better than to state that "some unknown portion" of individuals will seek initial or increased treatment making the potential economic benefits "difficult to quantity." The language further concedes that "figures on the number of individuals who avoid mental health treatment due to privacy concerns do not exist." Nevertheless, findings from a 1993 survey on health information privacy are cited: seven percent of respondents reported that they or a family member had chosen not to seek service for a physical or mental health condition due to fear of harm to job prospects of other life opportunities. The proposed rule goes on to acknowledge that the survey is "somewhat dated and represents only one estimate, " and that "there are other reasons aside from privacy concerns that led these individuals to respond positively." These shortcomings notwithstanding, the proposed rule makes some quantitative estimates based on additional arbitrary assumptions. For example, it is assumed that 5-25% of individuals that avoided treatment did so due to privacy concerns. It is further assumed that the treatment effectiveness rate would be 80%, again without any supporting evidence. Because of the questionable appropriateness of the survey results used and random assumptions made, little confidence can be attached to the dollar estimates of the benefits of the proposed privacy rule.

**Initial Regulatory Flexibility Analysis**

The text on p. 60036 says there are 1,078,020 small health care establishments, whereas Table A on p. 60037 says there are 448,498 small health care entities. This large

discrepancy is neither noted nor explained. Neither is there any mention of the difference between an ”establishment” and an “entity.” (The text also uses the term “enterprise.”) Table A presents other numbers that differ from the text, for example, in the case of hospitals, home health, and nursing facilities.

In Table B (p. 60037-8), the units in which dollars are expressed in the revenue columns are not given. Clearly, they must be some multiple of a dollar. Otherwise, one is left with the impression that average revenue per “office and clinic of doctors of medicine” is only $990 (i.e., $186,598,097 ÷ 188,508 from Table A).

**Economic Effects on Small Entities: the burden on a typical small business.**

This section presents estimates of the impact on small businesses of compliance with the proposed privacy rule. The conclusion is that system compliance costs for a small business would be $40.13 per entity, or 0.12% of expenditures in the first year and 0.05% (or 0.04% on p. 60043) of expenditures in subsequent years. All of the estimates follow a “top-down” approach, wherein an “industry total” estimate is divided by a “number of entities estimate” to obtain a “per entity” estimate. There are several problems with this method. First, it provides only a single point estimate and gives no indication of the variation around the estimate. A more serious drawback is that the top-down division approach is subject to numerous methodological errors. The entities to which the numerator pertains may not be the same entities to which the denominator pertains–a type of “apples and oranges” problem. If either or both the numerator and denominator are estimated with error (as they most certainly must be), there will be an error in the resulting quotient. Moreover, if numerator is underestimated and the denominator is over estimated (or vice versa), the error in the resulting quotient will be larger in percentage terms than the error in either the numerator or denominator.

The “top-down” estimates should be validated with a few “bottom-up” estimates, for instance, case studies of costs likely to be faced by a few individual providers/entities.

As they are, the estimates provided in the proposed rule seem absurdly low estimates of compliance cost impacts on small businesses. At a minimum, a survey of providers should be done to ascertain whether they believe a figure of $40 per entity per year is even in the ballpark.

**Unfunded Mandates**

The statement on p. 60044 that, “because the benefits of privacy are large, both productivity and economic growth would be higher than in the absence of the proposed rule” needs some explanation and elaboration, because it would seem that new regulations on businesses would inhibit productivity and economic growth.

**Collection of Information Requirements**

This section makes many assumptions regarding the impact on a health care entity of various provisions of the proposed rule. But, as with many other sections, the estimates are not generally supported by findings from studies. As such, they raise the same questions as to accuracy. It would have been better to do case studies on a few practices of various sizes in order to gain insight into how actual practices would be affected by complying with the proposed rule.

In conclusion, the AMA appreciates the opportunity to provide our considered remarks regarding the proposed rule for the Secretary's consideration. We particularly appreciate the extension of time granted for public comment to permit a thoughtful analysis. Our comments are extensive and we expect that other comments will be equally comprehensive. The AMA urges HHS to either (1) substantially revise the proposed regulation and reissue it as an interim final rule with the opportunity for comment, or (2) withdraw the proposed rule and issue a new NPRM. The AMA offers to continue to work with the Department to realize a final rule that will preserve patients' confidence in the health care system and their government's pledge to protect their privacy.

Sincerely,

E. Ratcliffe Anderson, Jr., MD

Cc: Gary Claxton, Deputy Assistant Secretary for Health Policy