February 17, 2000

Margaret Ann Hamburg, M.D.
Assistant Secretary for Planning and Evaluation
U.S. Department of Health and Human Services
Attention: Privacy-P
Room G-322A, Hubert H. Humphrey Building
200 Independence Avenue, SW
Washington, D.C. 20201

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

Dear Dr. Hamburg:

The American College of Physicians-American Society of Internal Medicine (ACP-ASIM), representing 116,000 physicians who specialize in internal medicine and medical students, is pleased to submit comments in response to the Notice of Proposed Rulemaking (NPRM) issued by the Department of Health and Human Services (HHS) and published in the *Federal Register* dated November 3, 1999. ACP-ASIM is in a unique position to evaluate patient privacy legislation: our members represent the gamut of internal medicine, including both general internists and subspecialists engaged in the practice of internal medicine as individual practitioners, members of group practices, government employees, professors of medicine, and medical researchers.

Summary of Comments

- We support the flexibility that would reject a "one size fits all" approach in implementing the privacy provisions, and the "minimum necessary" standard;
- We support the way the rule deals with disclosure of protected health information for research purposes, protecting patient privacy without imposing undue burdens that would impede research;
- We support providing patients with the right to inspect, copy and amend their patient records, and requiring notice to patients of their privacy rights and of how their medical information might be used or disclosed;
- We support the provisions regarding public health activities, health oversight, and judicial and administrative proceedings;
- In general, we oppose allowing the use and disclosure of confidential medical records without individual authorization for treatment, payment and health care operations (as defined in the NPRM);
- We are very concerned that the provisions on business partners would be very difficult to enforce, create open-ended and unpredictable liability for physicians and are unduly burdensome;
- We believe the provisions concerning law enforcement are too broad and would violate privacy rights;
- The costs of implementing the proposed rule have been vastly underestimated and would have a disproportionate impact on small business; and
- Physicians, especially those in small practices, will be subject to disproportionate administrative burdens as a result of the proposed rule, and should be exempted from the most onerous provisions of the rule. Physicians, unlike some of the other covered entities, are already bound by ethical obligations to uphold confidentiality and privacy rights of patients.

General Comments

Confidentiality is increasingly difficult to maintain in this era of computerized record keeping and electronic data processing, faxing of patient information, third-party payment for medical services and sharing of patient care among numerous medical professionals and institutions. ACP-ASIM commends HHS for tackling this difficult and complex issue and for attempting to ensure protection of patient confidentiality without impeding or preventing access to data that is essential to the efficient delivery of quality patient care and for medical, public health and health services research. Given the limitations on HHS's authority, the approach of trying to protect the information itself is understandable. We are concerned, however, that the proposal generally sweeps all covered entities together under the same complex regulatory framework. Individual physicians, governed by ethical codes of conduct and state professional disciplinary codes, are being lumped together with large institutional providers, health plans, and clearinghouses. Are there data to suggest that individual health care professionals are routinely and intentionally breaching confidentiality, or that patients fear that they are? Anecdotally, patients express concerns about health plans, organizations and institutions breaching confidentiality, not their individual physicians. Physicians are obligated to protect patient confidentiality, especially in light of the increased risk for invasion of patients' privacy from the computerization and electronic transmission of medical records. We are concerned that the rule, proposed as "a basic set of legal controls," might be viewed instead as all that is required of physicians, and could undermine the traditional ethical and professional obligations to uphold confidentiality. Moreover, the proposed rule does not cover entities that are more likely to wrongfully disclose and misuse confidential information.

The ACP-ASIM recognizes the need for appropriate safeguards to protect patient privacy, because trust and respect are the cornerstones of the patient-physician relationship and quality health care. Presence of trust, respect, and privacy create an atmosphere in which full disclosure of information from patient to physician can occur, enhancing treatment. Patients have a basic right to privacy that includes the information contained in their medical records. Medical personnel who collect health information have a responsibility to protect patients from invasion of their privacy. Patients need to be treated in an environment in which they feel comfortable disclosing sensitive personal information to a physician that they trust. Otherwise, they may fail to fully disclose conditions and symptoms, thereby reducing the effectiveness of treatment and perhaps seriously imperiling their health, or, they may avoid seeking care altogether for fear of the negative consequences that could result from a disclosure. Physicians have a responsibility to respect patient privacy first, except when doing so may result in serious harm to the patient or others, or when required by law. See ACP-ASIM Ethics Manual (Fourth Edition), Annals of Internal Medicine 1998, 128: 576-594). We are concerned that the NPRM goes too far in the direction of disclosure of protected health information without individual authorization; our concerns in this regard are set forth in more detail under the section dealing with "Treatment, Payment and Health Care Operations."

The NPRM is an important step in ensuring federal protection for the privacy of medical records and represents significant progress toward finding the right balance between the privacy rights of patients and the free flow of information that is necessary for the provision of effective and efficient health care services. The limited scope of HHS's authority pursuant to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, however, illustrates that comprehensive federal privacy legislation is needed. Because of the limitations imposed on HHS, too many burdens for compliance are placed on physicians. **While we are not suggesting that the medical privacy rule should not be applied to physicians, we do think that there should be a reexamination of the need for some of the provisions, as they would be applied to small physician offices. To the extent that small physician practices are not exempted from the provisions, HHS should apply them in the least burdensome fashion.**

Introduction to General Rules

ACP-ASIM supports the "scalability" approach taken in the NPRM, under which a "one size fits all" standard would be rejected for the implementation of the privacy provisions. It is critical that each affected entity be able to assess its own needs and devise, implement and maintain appropriate privacy policies, procedures and documentation to address its business requirements. Our members range from physicians working in solo practitioners' offices to multi-group practices to academic health centers, all of which have different needs and business practices.

ACP-ASIM also supports the stated general approach of the rule whereby protected health information (PHI) could not be used or disclosed by covered entities except as authorized by the individual who is the subject of such information or as explicitly provided in this rule. We disagree, however, with the actual approach taken by HHS whereby most uses and disclosures of an individual's PHI would not require explicit individual authorization (see discussion below).

Since Congress has not yet passed comprehensive confidentiality legislation, ACP-ASIM believes that special safeguards are needed to cover certain highly sensitive parts of a patient's medical record, such as HIV status, mental health disorders, drug and alcohol-related problems, sexually transmitted diseases, sickle-cell anemia, sexual orientation, and other highly sensitive health information.

Treatment, Payment and Health Care Operations

Subject to limited exceptions for psychotherapy notes and research information unrelated to treatment, a covered entity would be permitted to use or disclose protected health information (PHI) without individual authorization for treatment, payment or health care operations. The proposal would actually prohibit covered entities from seeking individual authorization, unless required by State or other applicable law. **While ACP-ASIM recognizes that this proposal is intended to make the exchange of PHI relatively easy for health care purposes and more difficult for other purposes, we are very concerned that this approach would allow the use and disclosure of confidential medical records without the consent of the patient in extraordinarily broad circumstances.** The proposed rule allow records to be shared without limit throughout the health care system; the confidentiality of medical records can be set aside for almost any reason at all. This approach undermines the bedrock principle critical to the physician-patient relationship of informed consent, and will undercut traditional codes of medical ethics.

Confidentiality between the doctor or other health care professional and the patient is an essential component of high quality health care. Physicians must obtain informed voluntary consent from the patient before their medical information is disclosed for any purpose, except for appropriately structured medical research (see below) or as required by law. (ACP-ASIM Code of Ethics; "Confidentiality of Electronic Medical Records," Public Policy Paper 2000). At some point in the treatment relationship between the patient and the physician, preferably at the first encounter, there should be some type of signed written authorization that is a legal, informed consent to the release of PHI for treatment and payment purposes. ACP-ASIM supports the approach taken in S. 578 (Jeffords-Dodd), e.g., some form of consolidated authorization by which health care providers and organizations can perform their various functions without having to stop and obtain authorization at every point in a patient's treatment. Consent is particularly important since the proposal generally would not restrict to whom disclosures could be made for treatment, payment or operations. When disclosures are made to non-covered entities (other than business partners), the protections afforded by this rule would not be applicable. While this limitation points to the need for passage of more comprehensive privacy legislation, until such legislation

is passed, individual's health information must be protected more strongly than provided under the NPRM.

Likewise, allowing disclosure of PHI without authorization for health care operations is problematic, given the broad definition of "health care operations." **As indicated above, ACP-ASIM supports requiring authorization before PHI can be used or disclosed for most health care operations. At the very least, the definition of what is considered to be health care operations should be narrowed to include only those activities that truly are related to treatment or payment.**

Minimum Necessary

ACP-ASIM agrees with HHS that a covered entity must make all reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure. Access should be limited to only those individuals who need access to the information to accomplish the use or disclosure. De-identified patient data should always be used in medical research and quality improvement processes, unless the nature of the research necessitates identification because coded data would be impracticable.

We support the use of firewalls to limit the possibility for improper data uses within an entity, but note that the proposed scalability standard is particularly desirable in creating barriers to access and review of PHI. Physicians maintain records in a variety of settings, from large academic institutions to private offices with two staff members who perform all administrative functions. Current conditions in medical offices typically place physical barriers between medical records and non-staff, as well as limiting business partners' access to records.

Practice management software and electronic medical record software packages are widely used by health care providers. Privately owned physician offices have limited access to technology with the capacity to create firewalls within their offices. Although software packages are available with a wide range of customizable features, they typically do not limit access on a field-by-field basis. Many programs limit access on a screen-by-screen basis or a function basis (such as appointment scheduling, billing, viewing laboratory results), but these are not completely customizable. Purchase of custom programming or replacement of current computer systems would represent an undue burden on providers who currently have as little as $300 or as much as $50,000 invested in computer software. Encryption technology is not currently available to most small businesses.

Proposed § 164.506(b) generally would place the responsibility for determining what is the "minimum necessary" disclosure on the covered entity making the disclosure. Covered entities would be required to make "reasonable efforts" and to incur "reasonable expense" to limit the use and disclosure of PHI. This standard, while flexible, when combined with the scalability approach leaves a health care provider's staff with a large amount of discretion and complete liability. It is not clear what "reasonable" means in this context; there is much gray area between what is "necessary" information for medical reasons and what is too much disclosure. In addition, a covered entity would be required to review each request for disclosure individually on its own merits, rather than institute a policy to approve certain types of requests. This provision will require that an individual with authority and knowledge to make "minimum necessary" determinations must review each record request. In small practices, page-by-page review of multiple record requests on a daily basis could pose excessive administrative time requirements. In many cases, it will be cumbersome to determine the exact need for every piece of information and exact measurement of information that may be required to meet that need.

We would encourage HHS to reconsider the excessive requirements placed upon clinical staff by transferring the burden of responding to medical record requests from clinical staff to administrative

personnel. Each hour of record review is deducted from the limited time that physicians and nurses are able to perform their primary functions, caring for patients. **Covered entities, particularly small businesses, should be allowed to create an internal policy to allow clerical staff to respond to many routine types of releases, including 1) disclosures allowed under any section of this proposed rule without patient authorization, and 2) any request accompanied by a written authorization signed by the patient. Moreover, the burden should be on the requestor of the information to make the "minimum necessary demand."**

Right to Restrict

ACP-ASIM generally supports the right of an individual to request that a covered entity restrict further uses and disclosures of PHI for treatment, payment or health care operations. However, administering a system in which some information is protected and other information is not poses significant challenges. In reality, this right will be severely hampered by health care providers' contractual obligations to insurers. Managed care organizations normally require that participating physicians not enter into private contracts for treatment and payment outside the physician's contract with the MCO. Thus, in its practical application, this right may be restricted to self-pay patients.

In cases not involving reimbursement, such as release to other physicians, providers may make good faith efforts to avoid those disclosures, but implementing security systems and tracking those limitations will be extremely difficult due to systems limitations. Electronic systems do not provide the capacity to exclude transmissions to particular providers. Physician office groups may request paper records and administrative staff may be unaware of the affiliation of a particular provider within that group. Tracking a myriad of restrictions may be impractical and could result in denial of all requests to avoid disclosure liabilities. **We would support providing examples in the final rule of appropriate, scalable systems that would be in compliance with this proposed provision.**

The Preamble notes that the proposed rule would not require a covered entity to agree to a request to restrict, or to treat or provide coverage to an individual requesting a restriction. HHS correctly recognizes that the medical history and records of a patient, particularly information about current medications and other therapies, are often very much relevant when new treatment is sought. Physicians have an ethical and in many cases legal obligation to treat a patient until that patient has been formally transferred to the care of another provider and/or discharged. **Provisions should be made to accommodate provider treatment and disclosure after the covered entity has refused a non-disclosure request.**

Creation of De-identified Information

ACP-ASIM supports the approach proposed in § 164.506(d) for de-identifying identifiable information and the use of restrictions designed to ensure that de-identified information is not used inappropriately. We believe that health information should be encrypted before being transmitted electronically for research purposes. For the majority of physicians in private practice, however, development and implementation of procedures for stripping identifiers will be cumbersome. A typical physician's office has neither the technical ability to create de-identified data nor the staff to manually de-identify data. **We support a "reasonableness" standard whereby entities with sufficient statistical experience and expertise could remove or code a different combination of information.**

Business Partners

We have major concerns with and strongly object to the business partner provisions. While we recognize the limitations imposed on the authority of HHS to directly regulate entities other than health plans, health care providers and clearinghouses, we are concerned that under the business partner provisions,

physicians would become regulators for HHS. These provisions would not only be unduly burdensome to physicians, but also would be exceedingly difficult to enforce. Physicians would be exposed to open-ended, unpredictable liability. Each of these concerns is discussed in further detail below.

Under the proposal, for purposes other than consultation or referral for treatment, covered entities would be able to disclose PHI to business partners only pursuant to a written contract that would limit the business partner's uses and disclosures of PHI. The contract between the covered entity and the business partner would be required to include certain provisions that are specified in the proposal. Each specified contract term would be considered a separate implementation specification under the proposal, and a covered entity would be responsible for assuring that the business partner meets each such implementation standard. These complex contract terms and new obligations will necessitate the investment of much more time and resources by medical and legal personnel. Business partners may incur substantial expenses in meeting privacy requirements, which could result in more expensive contracts for health care providers.

Non-compliance by a business partner or its sub-contractor of the terms of the contract could expose the physician to significant civil or criminal sanctions. Physicians would be in violation of the rule if they knew or "reasonably" should have known of a material breach of the contract by a business partner and failed to take reasonable steps to cure the breach or terminate the contact. Physicians would also be responsible for mitigating the harm caused by such violations. It will be very difficult, if not impossible, for most physicians to enforce the required contracts. No analysis has been done of the number of single-source business partners used by health care providers. A Medicare carrier acting as a fiscal intermediary, for example, would qualify as a business partner. However, HHS awards single-source contracts, leaving the physician with no viable alternative if required to terminate a contract. **These provisions, by making physicians liable for disclosures by others not under their control, raise serious questions of fairness, and should not be included in the final rule.**

Business partners will be impacted by the need to maintain business records for legal and/or financial auditing purposes. This may make the destruction or return of all PHI unlikely or impossible in certain circumstances. For example, billing services are subject to HHS audit. If business partners cannot maintain PHI, they cannot provide documentation of coding or submissions material, nor protect themselves from claims made against them related to bookkeeping errors. Computer back-ups that are maintained by many business partners might include PHI. Business partners cannot be expected to destroy all forms of electronic back-up just because they have completed work for one particular client. Outside entities that provide financial services and have access to information included on standard explanation of benefits forms will also be required to identify and destroy substantial numbers of documents. Such entities could include banking entities providing lockbox services, billing services, third-party medical collection agencies, third-party coding experts, consulting and auditing services and third -party claims processors, such as Medicare carriers.

Finally, and perhaps of most concern, a requirement included in the proposed contractual agreement would create a private right of action. Individuals whose PHI is disclosed by a business partner in violation of the rule would be considered to be third-party beneficiaries. As a third-party beneficiary, a patient would have a right under contract law to enforce the terms of the agreement by seeking damages against the breaching business partner and against the covered entity for failure to select and monitor properly the business partner. Covered entities would most likely have to purchase a rider under their insurance policies in order to be covered against such claims.

Uses and Disclosures with Individual Authorization

The regulation would require that covered entities have authorization from individuals before using or disclosing their PHI for any purpose not otherwise recognized by this regulation. ACP-ASIM supports the requirement that individuals must give specific authorization before a covered entity could use or disclose PHI for purposes unrelated to health care treatment or payment. (As discussed earlier, ACP-ASIM opposes disclosure of PHI without patient authorization except in limited circumstances).

We support the provisions in this section. Physicians must release information to the patient or a third party at the request of the patient. (ACP-ASIM Ethics Manual) Patient-initiated authorizations should be specific enough in terms of the information to be disclosed and to whom the information is to be disclosed to enable the physician to comply with the individual's request. Specific authorization is much better than the current practice of using broad disclosure forms. **ACP-ASIM supports requiring an expiration date as well as allowing authorization to be revoked by a patient unless action has been taken in reliance on the authorization.** With respect to authorizations initiated by covered entities, we support the requirement that the authorization form should identify the purposes for which the information is sought as well as the proposed uses and disclosures of that information. Patients need to be able to make informed decisions. Finally, we support the provision stating that treatment and payment should not be conditioned on a patient's authorization.

Public Health Activities

ACP-ASIM supports the provisions that would permit covered entities to disclose PHI 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 contacting or spreading a disease. Confidentiality may be overridden to protect the public health or individuals such as sexual partners at risk, or when the law requires it (e.g., mandatory public health reporting). However, before breaching confidentiality, physicians should make every effort to discuss the issue with the patient. (ACP-ASIM Ethics Manual).

Health Oversight

ACP-ASIM supports allowing disclosure or use of PHI without individual authorization for health oversight activities. **However, individual identifiers should be coded or encrypted whenever practicable.**

Judicial and Administrative Proceedings

ACP-ASIM supports permitting covered entities to disclose PHI in a judicial or administrative proceeding if the request for such PHI is made through or pursuant to an order by a court or administrative tribunal. A court order would not be required if the PHI being requested relates to a party to the proceeding whose health condition is at issue, and where the disclosure is made pursuant to a discovery order or is otherwise authorized by law. In the latter instance, however, we are concerned that the burden and possible liability is on physicians to determine whether the request relates to the PHI of a litigant whose health is at issue. Physicians and their staff are not best suited for making such determinations.

Law enforcement

The proposed rule would permit covered entities to disclose PHI without individual authorization to a law enforcement official conducting a law enforcement inquiry authorized by law if the request for PHI is made pursuant to a judicial or administrative process. We think that these provisions are too broad. Access by law enforcement officials to individual health records constitutes an inherent privacy violation. Health information is collected to provide quality care to patients and to help society through use of data in public health research. This information is not intended for law enforcement because of the potential for abuse. Access by law enforcement agents should be restricted to searches that are not open-ended and for which there is a just cause. **Release of confidential medical records to law enforcement officials should be permitted only when sustained by either subpoena or court order, except in limited emergency circumstances. Broad-based access is not an acceptable option. Law enforcement should be required to go through an independent review or neutral magistrate.** Administrative subpoenas may be issued based on an individual law enforcement request, sometimes without any higher review. **HHS should require that law enforcement officials obtain a judicial order**.

Research

It is critical that the provisions dealing with research recognize the precarious balance between protecting patient privacy and expanding on our knowledge of health and disease. Rules need to be structured so that they will not unduly burden health researchers in their quest to further public health and other vital medical research.

We generally support the way the proposed rule deals with research and the privacy of patient information. The proposal would permit covered entities to use and disclose PHI for research without individual authorization, provided that the covered entity receives documentation that the research protocol has been reviewed by an institutional review board (IRB) or equivalent body, and that the board found that the research protocol meets specified criteria designed to protect the subject. Absent such documentation, the subject's PHI could be disclosed for research only with the individual's authorization.

IRBs review research requests to ensure adherence to standards of patient protection and treatment in medical research. The boards are established to ensure that patients have been fully informed and that they have consented to their participation in clinical research. Any research using patient information – whether the information is identified or not, whether consent is obtained or waived – should be approved by an IRB. IRBs are an efficient and effective way to protect the rights and privacy of patients who consent to sharing their health information for the benefit of medical research. The conduct of research and the protection of patient confidentiality also must be in compliance with professional ethical guidelines and codes of conduct.

De-identified data should be used in medical research whenever possible, unless the nature of the research necessitates identification because coded data would be impracticable. All medical

research studies that use potentially individually identifiable information must contain measures to protect the confidentiality of individual patient records and should be examined and approved in advance by an IRB or similar ethics review board. IRB functions include carefully reviewing the type of patient consent needed within the context of each study. Additional protection for subjects should be required if the information is identified and the waiver of consent in these instances should be limited.

The use of data sets for secondary research studies should be allowed for statistical analyses and public health, but the records should remain encoded whenever possible. Patients, however, should be notified when information is to be used for purposes other than originally agreed on, and they should have the option to deny consent. These other purposes include billing, organizational research and quality improvement programs. Unfortunately, there is no clear line to differentiate between a routine use and a research use. Often, primary and secondary data uses overlap, and their definitions are dependent on the context within the individual studies. Uses of "de-linked" information require review by an IRB or other similar panel. While we recognize the limited authority of HHS over researchers who are not covered entities, **the ACP-ASIM believes that the burden for information requests should be borne by those requesting access to the information; we realize the need for stringent review in determining who has access to de-identified information.**

Notice of Information Practices

We generally support the provisions in this section that would require health plans and providers to give notice of their confidentiality practices and procedures to patients. Such notice would be intended to inform patients about what is done with their PHI and about any rights they may have with respect to that information. Notice is an essential component of giving individuals the ability to make informed choices about their medical treatment. **We support a flexible approach in allowing each provider to create a notice that reflects its own unique information practices.**

We do have concerns, however, about the administrative burdens and costs of such requirements, particularly for small practices. Small businesses are required to provide a notice of information practices on the patient's date of first service after the effective date of the rule. Determining the "first service" would place an undue administrative burden on many small practices. On a daily basis, staff would have to manually review each chart, or, in many cases, access a computer system to determine whether the patient has been seen since implementation of the rule. Internal medicine physicians average 4,000-5,000 patient charts; approximately 2,200 charts are considered to be "active." ("active" should be defined as those patients who have been seen in the last two years) The initial cost to produce, copy and mail notices could easily exceed the estimated $375 first year cost per provider office. Assuming 50 cents per authorization, the total cost could easily reach $1100 per provider in medical offices. Moreover, the cost attributed to tracking individual patient receipt of the notice would be extensive. These administrative costs would be incurred again whenever a notice is updated. **Physicians who mail notices to active patients, prominently display the notice and provide the notice to all new patients should be relieved of any additional notification requirements.**

Requiring signed acknowledgment of the notice, which in theory sounds like a good practice, in reality will only increase administrative burdens and costs. We also suggest a clarification to the provisions. The proposal does not clearly define the scope of initial notifications required. Will notification be required if the patient's last treatment date was prior to the rule's effective date?

Access for Inspection or Copying

Patients have a legal and ethical right to review information in their own medical records. In rare and limited circumstances, health information may be withheld from a patient if there is significant likelihood

of a substantial adverse effect on the physical, mental or emotional health of the patient or substantial harm to a third party. The onus is on the provider to justify the denial of access.

The proposed rule would allow, but not require, a researcher/provider to deny a request for inspection and copying of the clinical trial record if the trial is still in progress, and the subject-patient had agreed to the denial of access in conjunction with the subject's consent to participate in the trial. The IRB or privacy board would determine whether such waiver of access to information is appropriate, as part of its review of the research protocol. In the rare instances in which individuals are enrolled in trials without consent (such as those permitted under FDA regulations), the covered entity could deny access to information during the course of the trial even without advance subject consent. However, access during the trial would be appropriate if a participant has a severe adverse reaction and disclosure of information during the clinical trial would give the participant adequate information for proper treatment decisions. In all cases, the subject would have the right to see the record after the trial is completed. We agree with these provisions.

Access to current records within thirty days is reasonable for active patients. Medical records of patients last seen more than two years previously, however, may have been moved to off-site storage, which necessitates a longer recovery period (perhaps 60 days), and incurs additional cost. **We suggest that a structured extension procedure should be included in the final rule. We do not support requiring an acknowledgment procedure.**

Accounting of Disclosures

While we support in principle the requirement for an accounting of disclosures, we have several concerns about the proposal in its current form. First, covered entities would be required to provide an accounting of all instances where PHI is disclosed for purposes other than treatment, payment and health care operations. However, as currently drafted, PHI may be disclosed without individual authorization for those purposes. Thus, patients could learn who has had access to their PHI only when such information is disclosed with their consent, but they do not have such a right when consent has not been given. It would seem that it would be more important to provide an accounting for disclosures where an individual has not given prior authorization.

Second, we are concerned about the administrative burden and cost of complying with the accounting requirements. We agree that accounting should not be required for payment, treatment and most health care operations, but, as discussed earlier, we recommend that individual authorization should be required prior to the disclosure or use of PHI for such purposes.

Finally, we suggest amending section 164.515(c)(1)(v) to clarify that "copies of all requests for disclosure" refers only to individual-initiated requests.

Amendment or Correction

We support the right of patients to review the information in their medical records and to propose corrections. At the same time, however, it is critical to keep in mind that medical records provide working documentation for physicians and are often referred to in support of actions taken on the patient's behalf. The integrity of the medical record is critical. Therefore, medical histories should not be re-written or deleted. Physicians are liable to health plans for providing supporting documentation for all information submitted and requests for payment. If this information is later determined to be inaccurate, corrections can be made and submitted as appropriate. The original documentation, however, is still necessary.

Training

Many health care providers' employee training programs or employee handbooks currently incorporate confidentiality policies, so the additional burden imposed by the initial training requirement would be negligible. Re-certification, however, would impose a new administrative burden and is of questionable value when privacy policies remain unchanged. **Re-certification should be required only when a provider's privacy policy significantly changes.**

Safeguards

The proposal would require that a covered entity have appropriate technical and physical safeguards to protect the privacy of PHI. Medical records intermingle electronically transmitted data, non-electronically transmitted data, and data that is referenced in both formats. Therefore, providers most likely will have to presume that all records must be considered PHI and treated as such. Many small practices keep records in central areas easily accessible to all staff; such areas are not easily adaptable to "locked storage" areas. Replacement of an open medical chart storage cabinet with a lockable unit costs approximately $800 and provides little benefit. A typical physician has between three and ten units. **A small business should be required instead to provide physical barriers (e.g., walls or counters) to limit the access of non-authorized personnel to record storage areas.**

The proposal also would require a covered entity to verify the identity and/or authority of persons requesting PHI. This places an unusual burden on health care providers to verify requests that are normally received verbally or via fax. Moreover, ascertaining whether a requestor has the appropriate legal authority is beyond the scope of the training or expertise of most employees in a physician's office. **Health care providers must be able to reasonably rely on the authority of the requestor.**

Sanctions

We support the flexibility in the proposal that would allow covered entities to develop the sanctions policies appropriate to their businesses and operations. The ACP-ASIM supports holding users of electronic medical data accountable for protecting patient privacy. We are concerned, however, that a provider would be held liable for violations by a business partner and its subcontractors. As discussed earlier, **we think that there are fundamental fairness issues in holding providers accountable for the actions of another entity that they do not control.**

Small Business Impact

The NPRM does not propose a specific definition for small businesses, but incorporates the U.S. Small Business Administration's (SBA) baseline revenue definition for small businesses, which is $5 million in annual revenue. We do not believe that this proposed guideline, as currently defined, will include the projected 90% of health care providers. The Medical Group Management Association's Cost Survey Report for 1998 indicated that only 52.01% of group practices would not exceed the $5M revenue threshold. In addition, the SBA has proposed adjusting the revenue requirement for Doctors of Medicine (SIC 8011), as well as certain other health care-related providers, to $7.5 million. SBA has proposed this increase to reflect the disadvantage that health care providers face in a highly competitive market, even though their revenue has increased. We would encourage HHS to reflect this amended revenue standard in the final rule.

Additionally, we encourage HHS to consider establishing an alternative test for small businesses, based upon number of employees. Health care providers in particular areas of medicine, such as cardiology or oncology, would exceed the revenue requirements in a practice of four to five physicians. To achieve

parity across specialties with widely divergent average revenues, we encourage HHS to consider extending the definition of small business to any health care provider employing less than twenty employees. **This definition is supported by the report, "Employer Firms, Employment, and Estimated Receipts by Firm Size and Industry, 1996," issued by the SBA's Office of Advocacy, which indicates that 92% of Doctors of Medicine worked in firms with fewer than 20 employees.**

Conclusion

The proposed rule is an important first step in ensuring federal protections for the privacy of medical records. The ACP-ASIM appreciates your consideration of our comments and looks forward to working with you as the rulemaking process continues. If you have any questions, please do not hesitate to contact Debra Cohn, Legislative Counsel (202/261-4541) or Jack Ginsburg, Director of Policy Analysis and Research (202/261-4542).

Sincerely,

Whitney W. Addington, M.D., FACP
President