Position Paper

of the

AMERICAN COLLEGE OF PHYSICIANS -

AMERICAN SOCIETY OF INTERNAL MEDICINE

CONFIDENTIALITY OF ELECTRONIC MEDICAL RECORDS

April 29, 1999

"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. Physicians should be aware of the increased risk for invasion of patients' privacy and should help ensure confidentiality."

ACP-ASIM Ethics Manual (Fourth Edition)

The computerization and electronic transmission of medical records facilitates the flow of medical information, but it also raises many questions and concerns about security and protection of patient privacy. Health care information privacy rights, have, in the past, been protected through the physician's obligation of confidentiality. Today, new computer applications and new information technologies enable increasing amounts of

patient information to be readily accessible for physicians and other health care providers. If access to the data is granted, then this technology will also facilitate access to private patient information by utilization and quality reviewers, third-party payers, clinical and epidemiological researchers, but also to drug marketers, criminal investigators, and others.

Traditionally, physicians established and maintained possession of their own patient medical records, and were primarily responsible for preserving the privacy of their records. However, the change in health systems and the expanded use of technology in medical record keeping, both, increase concern about maintaining the security of confidential medical records. This issue is especially vital where socially stigmatized diseases (AIDS, alcoholism, drug abuse, and mental health issues) and genetic pre-dispositions information are involved because this information could be used by potential employers to discriminate against job applicants and by insurers to deny health insurance coverage.

Historical and Contemporary Overview

Currently, there are very few federal protections for the privacy of medical records. The Privacy Act of 1974 provides protection for personal information collected and held by the government. The Act prohibits federal agencies from disclosing identifiable information without an individual's "prior consent", except if the disclosure is "consistent with" the purposes for which the information was originally collected. The act also gives people the right to see, copy, and correct their records. In addition, the Department of Veteran's Affairs is bound by confidentiality rules covering the treatment

of drug and alcohol abuse, HIV and sickle-cell anemia. There is no federal legislation providing protection for privately held medical records.

However, a vast array of legislation dealing with confidential health information has been proposed at the state level and passed, in some form, in over 30 states. Several of these bills target protecting the confidentiality of medical records, without restricting medical research. For example, in 1998, Maine passed comprehensive privacy legislation that established safeguards for maintaining the confidentiality, security and integrity of health care information, while also requiring authorization by patients for disclosure of their health information. [(1)] Among the myriad of state-proposed legislation are proposals to cover disclosure of communicable diseases, protection of mental health records, requirements for managed care organizations to protect the personal health information of their members, requirements for encryption of electronic medical records, etc.

Congress attempted to address some of these privacy and security concerns when they adopted the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which directed the Secretary of the Department of Health and Human Services to develop recommendations and standards for protecting the confidentiality of medical records. The Secretary was specifically directed to develop a system of unique individual patient identifier numbers that would facilitate access and tracking of patient medical information for doctors, hospitals, payers, researchers, quality reviewers and other authorized persons/organizations. Congress gave itself until August 1999 to enact medical privacy legislation; otherwise the Secretary of HHS is authorized to promulgate regulations. In

September 1997, the Secretary issued a report containing recommendations for possible national standards. The National Committee for Vital and Health Statistics, an advisory body to HHS, also addressed the issue and held an open hearing in July 1998. Consequently, a series of proposed rules and regulations have been issued by HHS concerning a new HCFA system of records for measuring Medicare health plans, security standards, and electronic signature standards.

The issue of individual patient identifiers has generated substantial controversy. Having a unique, single ID number for each patient could facilitate access to vital information needed by physicians for treatment, particularly in emergency situations and for treating patients presenting without their previous medical records. The patient ID could enable the physician to check a complete patient history, including immunizations, allergies, medications, and possible drug interactions. Individual ID numbers would also facilitate quality reviews, health services research and epidemiological studies. Managed care organizations could also use the patient ID for tracking costs and for quality improvement studies. This increased access to data would require a central repository of all medical data collected from a health system that could be freely accessed by any authorized users, and possibly be accessed for other, non-authorized, purposes.

HHS has recommended that federal privacy laws create a floor, rather than a ceiling for protective legislation, leaving the states ample flexibility to adopt more stringent guidelines. This approach preserves the innovations that individual states have made in the past several years to protect their citizens from infringements on their privacy.

However, there is a compelling argument for implementing a single national system of legislation that will allow interstate health care providers and insurers to deal with one comprehensive regulation.

However, privacy advocates are concerned that the federal government will electronically link Medicare and other databases to create huge databases that allow anyone with access to be privy to every aspect of a person's medical history. They also fear that even if access is restricted to authorized persons with legitimate needs for information, current security measures may be inadequate to prevent computer hackers and others from invading patients' privacy. Consequently, several members of Congress proposed legislation to repeal the provisions of HIPAA and to stop further efforts to assign individual patient identifiers. In response, Vice President Gore announced late in July 1998 that the Administration would not proceed with its plan to implement a system for individual patient identifiers until Congress passes legislation to protect the confidentiality of medical records. Although medical records confidentiality legislation has been considered by Congress both as part of various patient protection bills and also separately, as of early 1999, Congress had not yet passed legislation dealing further with the issue.

In addition, in October 1998, the European Union adopted a directive requiring that all countries adopt privacy control laws if they wish to share patient medical information for the purposes of research. This directive raises particular concerns for American companies and health care organizations that rely upon members of the

European Union for medical information and creates a further impetus for privacy legislation.[2]

Patients' Right to Privacy

Position 1: Patients have a basic right to privacy that includes the information contained in patient medical records. Medical personnel who collect health information have a responsibility to protect patients from invasion of their privacy.

Patients have a basic right of privacy. The very nature of medicine depends on the physician-patient relationship. 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 negative consequences that could result from a disclosure. Physicians have a responsibility to respect patient privacy first, except where doing so may result in serious harm to the patient or others, such in the non-reporting of communicable disease that may pose a risk to the patient and third parties. Physicians may, in very limited circumstances, breach confidentiality, if harm to a third party is foreseeable - for example, a breach in confidentiality is mandated in reporting certain

communicable diseases in cases where the patient is a danger to others, and in other situations such as child and spouse abuse. The duty to warn also extends to a patient's sexual partners when that patient has syphilis or is infected with HIV. Physicians are also required to disclose information when the law requires it.[2]

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 where full disclosure of information from patient to physician can occur for the better outcome of treatment.

Access To Medical Records

Position 2: The primary purpose of patient medical records is to document the patient's case and communicate information about patient care to health professionals involved in the treatment and care of that patient.

Position 3: Access to information in medical records should be restricted to persons with legitimate needs for the information.

Position 4: Patients have a right to review information in their medical records and to propose corrections.

The medical record is a tool used to provide an accurate record of the clinical diagnosis and treatment of patients. Ethically and legally, patients have a right to know what is in their medical record, except in circumstance where knowledge of medical information may be felt to harm the patient. Legally, the actual chart is the property of the physician or institution, although the patient generally has a privacy right in controlling information discoveries; thus, the dictum that "information should only be released with the written permission of the patient, or the patient's legally authorized representative."[3][4].

In rare and limited circumstances, health information may be withheld from a patient if there is a 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 lies on the provider to justify the denial of access.

Consent

Position 5: Informed consent must be obtained from patients before their medical information is disclosed for any purpose, the only exception being for appropriately structured medical research (see positions 7-9) or as required by law.

Position 6: Disclosures other than for healthcare-related needs should occur only as required by a court order.

Consent is to be obtained for all purposes, including treatment or payment. While it may be acceptable to disclose information in the context of a consult or to forward information for reimbursement purposes without the explicit consent of a patient, it is ethically required that the patient be told up-front of such a disclosure. Communication between a consultant and the referring provider or primary care provider is implied in the referral and does not require written consent. A patient may at any time withdraw consent for disclosure of medical information, notwithstanding the financial consequences of third-party payer contracts to the patient or physician. However, the patient may have to assume responsibility for payment if the implied consent is withdrawn.

For physicians to disclose any information in a patient's medical record, the physician must obtain the informed, voluntary and non-coerced consent of the patient, especially when the disclosure is not related to treatment or payment. Realizing that integrated health care systems require certain data for treatment and the processing of claims, there needs to be a basic level of patient consent to ensure that these activities can be performed. ACP-ASIM supports the creation of protections whereby those in managed care settings who are responsible for billing and payment only have access to the information needed to perform their functions and are not privy to all medical information contained in a patient's record.

Informed consent must always be sought by the physician, but in some very limited circumstances, information can be disclosed without consent having been obtained. Exceptions are justified if the information is being used for medical research with adequate safeguards to protect patient privacy (see positions 7-9), or is required by law (see position 10), as in the case of mandatory public health reporting, under emergency conditions.[6]

Access for Research and Quality Improvement

Position 7: 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.

Position 8: If de-identified data is to be used for purposes other than those for which it was originally intended, patients must give additional consent.

ACP-ASIM advocates the development of guidelines on the kinds of access researchers should have to these records, as well as when identified data is needed. De-identified data should be used whenever possible. If a study requires patient identifiers,

then appropriate safeguards must be firmly in place. A case can be made that a unique identifier could be a useful way to better secure patient identity because that unique identifier would create a more efficient linking/de-linking system for data storage. The more "unique" identifiers that exist for an individual, the more data systems have to institute quality assurance checks to assure themselves that records are not duplicated or missing. This can lead to the excessive scrutiny of records (such as relinking) which can increase the risk that data analysts see individual records as they determine whether a record number is the same as the patient number. A unique identifier would keep this kind of activity to a minimum and would create a system that would create quality research that assures patient confidentiality.

The use of datasets for research for secondary research studies should be allowed for statistical analyses and public health, but the records should remain encoded when possible. However, patients should be notified when information is to be used for purposes other than originally agreed upon and, they should have a further option to deny consent. These "other purposes" include, but are not limited to, billing, organizational research and quality improvement programs. Unfortunately, no clear line exists to differentiate what is a routine use from what is considered a research use. Often, primary and secondary data uses are overlapping and their definitions are dependent on the context within the context of the individual studies. ACP-ASIM believes that uses of de-linked

information require review by an appropriate authority, such as an Institutional Review Board or other panel set up in an administrative setting.

ACP-ASIM believes that the burden for information requests should fall on those requesting access to information, and we realize the need for stringent review in determining who has access to de-identified information.

Position 9: Disclosure of health information should be permitted only for research that is approved by an Institutional Review Board and is in accord with federal policy for the protection of human subjects.

Institutional Review Boards (IRBs), or ethics review boards, review research requests to ensure adherence to standards of patient protection and treatment in medical research. The boards are established to assure that patients are fully informed and consent 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. IRB's 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.

Studies that use potentially identifiable information must continue to be examined and approved in advance by ethics review boards. IRB functions include the careful review of the type of patient consent needed within the context of each study.[7]

Additional protection for subjects ought to be required if the information is identified, and the waiver of consent in these instances ought to be very limited, as suggested by the many requirements proposed by the Department of Health and Human Services.

However, if comprehensive confidentiality legislation is not passed by Congress, additional protections will be necessary to guard against discrimination that patients may encounter when seeking employment or health insurance. Special safeguards are needed to cover certain highly sensitive parts of the patient's medical record, such as a patient's HIV status, mental health, drug and alcohol-related issues, STDs, sickle-cell anemia, sexual orientation, and other highly sensitive health information.

NIH recently reported that "IRB-based human subjects protection programs has been implemented consistent with the regulations and continues to provide an adequate level of protection at a reasonable cost." The chairs of IRBs nearly unanimously agreed that their own IRB protected the rights and welfare of human subjects. The most common deficiencies found in protocols related to the consent form, which are often in excessively technical language."[8]

The Canadian Medical Association (CMA) requires that any existing or proposed secondary purpose for health information collection, use, disclosure or access, including health information systems or networks, shall be subjected to patient privacy impact analysis that shall include an evaluation of:

(a) the likely impact of the proposed measures on the right of privacy of patients

(b) the likely impact of the proposed measures on the relationship between patients and their physicians, and in particular on the duty of confidentiality and the trust within this relationship

(c) the likely impact on the proposed measures on the willingness of patients to disclose health information.

(d) the likely impact of the proposed measures on the ability of patients to receive health care and

(e) compelling evidence to demonstrate broad public support for the proposed measures

IRB's could perform these measures and tests to ensure the protection of the confidentiality of medical records. ACP-ASIM supports IRB use of a balancing test to determine the utility of an activity (e.g. quality assurance and improvement) with the above-mentioned privacy considerations.

Along the same lines, the Secretary of the U.S. Department of Health and Human Services has recommended that disclosure of health information without patient consent should be permitted for research only for the following specific conditions:

- The research would be impracticable to conduct without the individually-identifiable health information;
- The research has been approved by and institutional review board (IRB) in accord with the Federal Policy for Protection of Human Subjects;

- An institutional review board has determined that disclosure in allowable without the informed consent of subjects and in making that judgment has determined that:
    - ♦ The research project is of sufficient importance to outweigh the intrusion into the patient's privacy; and
    - ♦ The research is of minimal risk; and
    - ♦ Not obtaining consent will not adversely affect the rights or welfare of the subjects; and
    - ♦ The research could not practically be carried out if consent were required.

We agree with each of these conditions. All medical research studies that require individually identifiable data must contain measures to protect the confidentiality of individual patient records and should be subject to approval by an IRB or similar ethics committee prior to the start of the study. The conduct of research and the protection of patient confidentiality must also be in compliance with professional ethical guidelines and codes of conduct.

Access for law enforcement

Position 10: Disclosure of health information for law enforcement purposes should require a court order.

HHS recommended that law enforcement officials continue to have virtually unlimited access to individual health records. However, ACP-ASIM believes that law enforcement access to this information 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 where there is potential for abuse. Certainly, access by law enforcement agents should be restricted to searches for which there is just cause and should not be open-ended. Release of confidential medical records to law enforcement officials should be permitted only upon presentation of either a subpoena or court order. Broad-based access is not an acceptable option.

UNIQUE INDIVIDUAL PATIENT IDENTIFIERS

Position 11: ACP-ASIM believes that the current dangers of a breach in confidentiality currently outweigh the limited benefit of national unique patient identifiers.

Position 12: Federal privacy protections need to be in place before implementing a national system of unique identifiers.

Position 13: If unique identifiers are created, every possible measure should be taken to ensure the security of this information.

HIPAA (Health Insurance Portability and Accountability Act) requires that the Secretary of HHS adopt standards to support the electronic exchange of a variety of administrative and financial health care transactions, and could likely extend to the exchange clinical information in the near future. Among the standards, are unique identifiers for all patients. HIPAA recognized the unique identifier for individuals as an essential component of administrative simplification. However, the idea of national unique patient identifiers has raised many questions regarding the right to privacy and the "Big Brother" aspect that this will impose on health care.

The Consumer Bill of Rights and Responsibilities which was published in November 1997 by the President's Quality Commission, highlighted the importance of confidentiality of identifiable health information. The President stated that, "Consumers have the right to communicate with health care providers in confidence and have the confidentiality of their individually identifiable health care information protected…"

In response to the growing controversy, Vice President Gore announced late in July that the Administration would not proceed with its plan to implement a system for individual patient identifiers until Congress passes patient confidentiality legislation.[9]

Despite this apparent embargo against the implementation of the use of individual patient identifiers, HHS is proceeding to develop a series of standards for the protection of electronic medical records. HHS has proposed standards for the security of individual health information and electronic signature use by health plans. Among these standards are uniform transactions and data elements for health claims, unique identifiers for individuals, standard language, classification systems for data elements, electronic transmission and authentication of signatures. Security standards would be used to develop and maintain the security of all electronic individual health information.

The security regulations would apply to all computerized transactions and the law would apply to each health care provider when transmitting or receiving any of the specified electronic transactions. The security regulation would apply to each health care provider electronically maintaining or transmitting any health information pertaining to an individual. The idea of an electronic signature is to establish a system of accountability in those who transmit information electronically. The department defines electronic transfers as including all media, even when the information is physically moved from one location to another using magnetic tape, disk, or compact disc media, Internet, Extranet, leased lines, dial-up lines and private networks.

Though the department suggests security standards, it does not recommend any specific techniques or technology stating that this is due to the quickly changing security technology market. They do concede, however, that the standard must be comprehensive.[10] ACP-ASIM supports a reexamination of this issue as technology continues to make advances to ensure that privacy will continue to be protected. The College will be able to support the idea of unique patient identifiers as soon as the technology becomes sophisticated enough to ensure patient protection.

Positive Aspects of Individual Patient Identifiers

In an increasingly mobile society, individual patient identifiers would allow records to be easily transferred to many providers. This system would help assure continuity of care and would facilitate ordering tests and reporting results, retrieving medical records and integrating information across various internal information systems. The ID number would facilitate access to vital information need by physicians for treatment, especially in cases of emergencies and for treating new patients presenting without their previous medical records. A unique patient identifier could enable the physician to check comprehensive patient records concerning patient history, immunizations and other preventive health services, allergies, medication, possible drug interactions and other data.[11] Unique identifiers could also aid epidemiology studies; especially research agendas that examine trends of large groups of people over an extended period of time.

Negative Aspects of Individual Patient Identifiers

Critics of individual patient identifiers warn against an increased danger for breaches of security and consequent inappropriate access to confidential patient information. A unique patient identifier heightens the risk of unauthorized access to private medical records, especially as medical records are transmitted electronically for payment, utilization review, audit and other purposes. Safeguards to protect confidentiality include encryption to prevent unauthorized access during transmission, but may be there is great concern among physicians and patients that such safeguards are inadequate and that encryption could be breached by computer hackers.

This controversy illustrates the need for federal privacy legislation to be in place before we can rule on the best way to provide unique identifiers to patients. Any identifier that may eventually be agreed upon needs to be subject to careful testing and risk evaluation to ensure that the maximum amount of privacy is granted while still allowing access to the information needed by health researchers.

Position 14: If individual patient identifiers are employed, they should not be linked to Social Security numbers.

Linking the unique identifiers to Social Security numbers has generated considerable discussion. However, this has the potential to link a person's health information with their credit and financial data. Many state governments, universities, and other private organizations currently use Social Security numbers (SSNs) for identification purposes. This health information could be subsequently linked to any number of things that are distinctly not health-related, such as motor-vehicle records and other civil events. In fact, there are federal laws that now require that SSNs be used in the administration of some programs, including the federal personal income tax program; Medicaid and Food stamps, state commercial driver licensing programs, etc. Many personal business also routinely choose to use SSNs to conduct their business or program activities.

Some contributors to this debate, such as the Computer-Based Patient Record Institute, believe that this link of health information with other data connected to Social Security Numbers is essential. They note the benefit of having access to a simple, already unique number, which most people have had since birth. In this scenario, the Social Security number would be equipped with a check bit, which is a series of additional characters at the end of the common-known nine-digit current number.

Before we create a new system that potentially merely replicates Social Security numbers and that might be extremely expensive, we must first examine whether a new system will provide a more secure system of unique identifiers. Although ACP-ASIM opposes development of unique patient identifiers, if a unique identifier system is created, the number should not be a person's Social Security number. Too many non-health

people already have access to Social Security numbers and people outside the health professions should not have access to personal health data.

Position 15: Health information should be encrypted prior to electronic transmission outside a physician's office for research purposes.

Currently, there are no accurate data on the number of break-ins that computer bases endure. Disturbingly, the General Accounting Office reported that the Department of Defense's computers received 250,000 attacks and that 65% of the attacks resulted in successful break-ins. The same report stated that the number of attacks appears to be doubling each year.[(12)] Even when the break-ins are discovered, people are hesitant to disclose such information. One safeguard would be to develop a secure encryption system. Physicians could continue to maintain their own medical records as desired, but data transmitted electronically would have to be encrypted. Only persons with legitimate needs for access to private medical data would be authorized to unscramble encrypted electronic medical data. This might work with authorized passwords much like access to secure sections of a computer website, but ACP-ASIM is skeptical that this can actually be implemented in a way that provides protection to our patients and their sensitive medical information. De-encryption keys or devices have also been proposed. There are ways of protecting against, or mitigating, the probability of intrusion or data theft. Some useful technologies include firewalls, communication channel encryption, and strong

password systems. However, current technology has not been able to create an infallible system—passwords can be stolen and encryption software can fall into the wrong hands which would invalidate an entire system. The College supports the research and development of altering these existing technologies to fit the requirements for health data protection. Nevertheless, it must be recognized that even the security of encrypted data is subject to breeches by determined computer hackers. Consequently, there must be strong penalties for those who violate patient privacy protections.

Penalties for Unauthorized Use

Position 16: Any person found violating patient privacy should face strong penalties including monetary fees and criminal charges.

ACP-ASIM supports strict criminal and civil liability for those found using the information for uses other than its intended purpose. HIPAA specifies penalties for misuse of health identifiers or for wrongfully obtaining or disclosing individually identifiable health information. The penalties, which increase by type and offense, can be as much as $250,000 and 10 years in prison. More serious offenses are defined as those committed under false pretense or those committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or

malicious harm.[13] The buying and selling of patient data, for example, for drug marketing is unconscionable. Patients need to be reassured that their health information will not be used in this fashion. ACP-ASIM supports holding users of electronic medical data accountable for protecting patient privacy and supports keeping track of who is authorized to use confidential health information. Criminal penalties should be imposed for violating confidentiality protections, for inappropriately using decoded data, and for deliberately corrupting data.

Conclusion

ACP-ASIM encourages the continued development and expansion of computerized medical record keeping and seeks to further facilitate the electronic exchange of medical information and health care providers and those with legitimate needs for health care data. However, the College also seeks to assure that patients' rights to privacy are respected and that the confidentiality of medical records is appropriately safeguarded. ACP-ASIM is particularly concerned that adequate privacy protections must be in place before any national system of unique patient identifiers is utilized for medical records. At this time, we believe that the dangers of breaches of confidentiality outweigh the benefits of developing unique patient identifiers. We are opposed to utilizing Social Security numbers for linking patient health information. The College is also keenly aware of the value of

medical research and the need to maintain access to medical records for research purposes. Accordingly, we have enumerated specific conditions that emphasize use of non-identifiable patient data whenever possible but that also permit access to identifiable data that is necessary for certain kinds of epidemiological research. We favor the development and use of means of encryption to protect the confidentiality of electronically transmitted data, and urge strong criminal and monetary penalties for those who violate patient privacy protections or misuse confidential health information.

There are a number of unresolved issues germane to the problems of patient confidentiality that may need to be considered in a subsequent paper. These include, but are not limited to:

- Problems of preemption of state regulations by a national policy
- Limitation of oversight by IRBs during the later stages of an ongoing longitudinal research protocol when follow-up requires de-identification
- How and by whom judgment is made that the project is of sufficient importance to "outweigh the intrusion into the patient's privacy"
- Need for an oversight mechanism for commercial usage of patient data arising from non-institutional research protocols (that usually no IRB approval and fall outside the "Common Rule" that requires IRBs for federally-funded research)
- The question of how to monitor privacy issues arising from limited informed consent
- Problems related to limited access of care givers to portions of the medical record

- How to write legislation which establishes penalties without the necessity for extensive legislation which would have a chilling effect on research

---

[1] Herstek, J. Issue Brief, Health Policy Tracking Service. Subject: Finance, Pharmaceuticals, Providers. Title: Medical Records. Accessed December 1998.
[3] Ethics Manual, American College of Physicians, Annals of Internal Medicine 1998: 128: 576-594.
[4] Ethics Manual, American College of Physicians, Annals of Internal Medicine 1998: 128: 576-594.
[5] Cognitively Impaired Physicians. American College of Physicians. Annals of Internal Medicine 1989, 111:843-8.
[6] Goldman, J. Protecting Privacy to Improve Health Care, Health Affairs, vol. 17, no. 6, November/December 1998: 47-60.
[7] International Society for Pharmacoepidemiology: Data Privacy, Medical Record Confidentiality and Research in the Interest of Public Health, August 18, 1997.
[8] Association of American Medical Colleges, Washington Highlights, vol. 9, no. 26. July 2, 1998.
[9] Department of Health and Human Services, Unique Health Identifier for Individuals: A White Paper. Accessed at http://aspe.os.dhhs.gov/admnsimp/nprm/noiwp1.htm
[10] Federal Register, vol. 63, no. 155, 8/12/98.
[11] Board of Governors Report, Medical Information Privacy and Security Act, Resolution 135, approved September 1998.
[12] Information Security—Computer Attacks at Department of Defense Pose Increasing Risk (GAO/AMID-96-84) 1996.
[13] Department of Health and Human Services, Unique Health Identifier for Individuals: A White Paper. Accessed at http://aspe.os.dhhs.gov/admnsimp/nprm/noiwp1.htm