Analysis and Commentary

American Psychiatric Association Resource Document on Preserving Patient Confidentiality in the Era of Information Technology

In 1987, the American Psychiatric Association Guidelines on Confidentiality noted: "[w]ith the development of computerized information networks to process certain aspects of medical records, the potential for harm to confidentiality is considerable." Three measures were recommended at that time: (1) extreme care should be taken to guard against inappropriate access to computerized information, (2) security safeguards should be implemented and tested, and (3) the electronic transfer of data between information systems should be limited to only that which is necessary for the purpose involved and the disclosure of information should otherwise abide by the same standards as the transfer of written material. Special concern was raised about the transfer of medical data into nonmedical information systems. "The psychiatric profession," wrote the drafters of the Guidelines, "has a responsibility to limit the amount of information transferred into such systems, to help monitor them and to educate the public about the potential dangers involved."

In the decade since the Guidelines were issued, the new information technologies have grown explosively and have been applied to medical practice in ways unforeseen even a few years ago. These developments have broken down the barriers to access that have traditionally protected patient information. In some settings, technology advances have obliterated the distinctions between records

This resource document was prepared by the American Psychiatric Association's (APA's) Committee on Confidentiality and the Council on Psychiatry and Law and approved by the Board of Trustees in December 1996 as a resource to the APA's District Branches. This document does not represent official policy of the American Psychiatric Association.

kept in private practice, psychiatric clinics and hospitals, and general hospitals and multispecialty clinics that were important a decade ago.

Historically, the appropriate handling of medical information has been addressed as an aspect of physician-patient relationships. Against the backdrop of a general expectation of confidentiality, professionals developed standards for maintaining records and disclosing information. In emerging health care systems, the traditional physician role as guardian of patient privacy is under serious attack. Traditional relationships between physicians and patients have been altered so that physicians may no longer be able to control medical information in the ways they once did. Moreover, new information technologies have enhanced the value and potential uses of medical data; as a result, third-party demands for access have increased, with attendant risks to patient privacy. Medical data are increasingly being used for nontraditional purposes (i.e., for purposes other than clinical assessment or treatment) that are unregulated by law or professional custom. Too often, new laws proposed to address medical record confidentiality have been inadequate. Some legislative proposals actually would undermine traditional protections of confidentiality that exist in state law and professional codes of ethics and practice. These bills would legitimate inappropriate uses of medical information, rather than protect patient privacy.

The developments in information technologies and systems pose challenges to psychiatrists, health care entities, and policy makers to adopt appropriate rules to protect patient privacy. In the next section, the problems raised by these new technologies and systems of care are discussed. Finally, principles to guide the crafting of rules and procedures regarding medical information (i.e., all information generated as a consequence of a physician-patient encounter) are presented.

New Information Technologies

Traditional medical record keeping poses substantial obstacles to intruders. Those seeking to inspect records must have authorization and view records in person. Moreover, because paper records are not centralized—a single patient's records may be fragmented across a number of physicians—in the event of a breach in security, illicit access will be limited. Indeed, patients who are especially concerned about privacy may seek services away from home or from their regular physicians in order to compartmentalize medical information.

Electronic information systems are intended to surmount physical barriers to accessing patient records and to facilitate the marriage of data from diverse sources into an integrated medical dossier. The potential utility of such systems are obvious and have been widely discussed. Nonetheless, electronic records pose inherent threats to privacy. Electronic storage of medical information opens the potential for access to the universe of people with the ability to gain entry to the data bank. Through remote access, patients' records may be viewed anonymously, and, once access is gained, comprehensive information may be available. The

threat to privacy is increased by computer technologies that free users from case-by-case browsing. In the time necessary to read a single medical record, thousands of computer files can be scanned or simply copied for later inspection. Even greater privacy invasions may result from the application of scanning programs that employ artificial intelligence to search files in order to identify records of interest. Moreover, when medical records are linked to other electronic data bases (e.g., social security, automobile registration, financial records including credit card purchases, bank records, and credit rating) the scope of potential intrusion by artificial intelligence is even larger. These information technologies make it possible for more people to know more about the private lives of others.

Some computer system experts believe that adequate measures can be implemented to assure patients' privacy. For example, health care systems can adopt policies and procedures that restrict access to information to those within the system appropriately. Moreover, security measures can be adopted to guard against illegitimate access. For example, data can be encrypted, and computer information systems can be designed to require passwords and to create audit trails automatically.

Many experts, however, believe that privacy is jeopardized whenever sensitive information is maintained in a computer data base. Inappropriate access by those within a defined system may be particularly problematic. Modern health care systems may include thousands of physicians, tens of thousands of support staff and ancillary personnel, and millions of patients. Policies may be written to permit broad access to those within the system, thus permitting illegitimate perusal of medical information. There is an inherent tension between procedures that facilitate access to an integrated electronic medical record system and those intended to protect patient privacy. Moreover, security measures may be breached. Users may share their passwords with others or may take inadequate steps to maintain secrecy. Encryption codes may be broken. And audit trails, while holding promise for the detection of unauthorized access, do not prevent invasions of privacy. Indeed, there are some information experts who believe audit trails are of little value because there will be so much data generated that it will be impossible to identify inappropriate security breaches. Security measures have been notoriously ineffective in preventing inappropriate access from those outside computer data systems.

Increased Complexity of Health Care Systems

Patients enter treatment and disclose private information about their health to physicians with the expectation that what is disclosed will be used to benefit their present and future treatment. Traditionally, health care systems have maintained records solely to serve the medical interests of care and treatment. Physicians, acting in the interests of their patients, have served as the guardians of patient confidentiality and have controlled access to medical records. As the guardian of confidential medical information, physi-

cians have protected patients' privacy from unwarranted intrusions that might result from unauthorized or authorized disclosures. When information is sought by others, physicians refuse inappropriate access. When the right to access is uncertain, physicians have acted as sentinels, alerting patients that others are seeking their records. Physicians may take steps to protect records even in the face of legal pressures. Moreover, physicians, aware of the misuses of medical information by third parties, have offered guidance to patients so that voluntary disclosures of medical information are tailored to meet the needs of third parties and minimize privacy intrusions.

As health care systems have become more complex, medical information has increasingly been put to uses that are not intended to serve patient interests. Initially, insurers gathered medical information to validate claims, to ensure that they were billed appropriately. However, in recent years, medical information has been put to commercial uses as well. In some instances, diagnostic information may be sold to direct marketers of health-related products. The most disturbing use of these data banks is to determine individuals' risk ratings. In these cases, individuals may find that information that they have conveyed to their physicians with the expectation that it will be used to benefit them is used to deny access to health care coverage—contrary to their medical interests. Moreover, treatment data may be used to deny access to disability or life insurance for the patient, or family members who are genetically at risk.

Principles

The Guidelines issued in 1987 were intended to aid practicing psychiatrists and, for the most part, remain current. The following principles are intended to update the Guidelines and to provide direction to policy makers as they lay the ground rules for the management of patient records in electronic form in new health care systems.

1. Patients—or parents or guardians when appropriate—have a right to be notified about how their medical data will be recorded, stored, and used. Many patients are unfamiliar with computerized record keeping and may be unaware that their private medical information can be stored in computer files, electronically transmitted, and accumulated in shared insurance data banks. Because new information technologies may pose special risks to privacy, patients should be notified when their medical data is stored in a computerized or electronic form. Insurers, including government entitlement programs, should inform patients about the routine information required to validate claims, and how this information is obtained, handled, and stored.
2. Medical data are generated for the care and treatment of patients and should be used to serve their interests. In order to preserve the integrity of record keeping as a clinical tool in new information systems, policy makers should implement the following recommendations.
   A. Psychiatrists must continue to be the guardians of medical informa-

tion. Psychiatrists—as well as other physicians—have ethical and legal responsibilities to act in their patients' interests and are in a unique position to understand patients' privacy and other interests. Therefore, psychiatrists must continue to play an active role in ensuring that the security of medical data is maximized in health care systems. Moreover, as noted in the Guidelines, psychiatrists operating in health care systems "should take care to limit the information contained in the medical record to the minimum that is required for good care and documentation." However, for some patients' records, the potential damage of inappropriate disclosure of even minimal information may be so great that the additional risks associated with electronic storage cannot be justified. In new systems of health care, psychiatrists—in consultation with their patients—must be able to determine which information safely can be entered into computerized or electronic forms. Psychiatrists should be able to record sensitive information in a secure, personal work file as a means of protecting privacy if the security of computerized data is unacceptable to their patients.

Health care systems, insurers, and policy makers must be sensitive to privacy concerns and, where feasible, should provide alternative, traditional methods of record keeping. Concerns about the privacy of computerized medical information may be minimized if systems can demonstrate a track record of maintaining appropriate security. Various approaches to enhancing security may prove useful. While all health care information should be maintained confidential, security may be enhanced by compartmentalizing certain kinds of data and limiting access to sensitive information within systems. Those who enter a given patient file would have access to some, but not all, of the recorded information absent patient consent, emergency, or other specified circumstances. Because health care facilities and information systems may differ in important ways, it is not possible to identify a single security scheme that will best serve the needs of patients in all settings. One possibility is to allow patients and the responsible physicians to identify information that is to be kept under special security and to specify the conditions for access. Alternatively, a health care system may establish secure compartments based on diagnoses (e.g., psychiatric disorders), treatment (e.g., psychotherapy notes), or location (e.g., physicians at one HMO site may have access, but no remote access by physicians at other sites). In general, the psychiatric profession must strongly support policies and procedures that are non-discriminatory with respect to the treatment of psychiatric and non-psychiatric medical disorders. However, psychiatric patients and treatments continue to be subject to societal stigmatization and psychiatric patient records may be more likely to contain sensitive information. Psychiatrists must

support a system that best fits the needs of the patients in their particular setting.

Mechanisms for the release of information from health care information systems must include provisions that permit the exercise of professional medical judgment in disclosure decisions. As discussed below, professional judgment may be exercised by direct involvement of psychiatrists in decision making regarding each disclosure. Alternatively, psychiatrists, along with other physicians, may exercise necessary professional judgment through the implementation of disclosure policies that govern the actions of medical records personnel and others in the system. However implemented, psychiatrists must be able to fulfill the role of guardian of the record. Third parties may seek information without authorization or other legitimate purpose; alternatively, they may request unnecessarily extensive or detailed information. Patients inadvertently may sign release of information forms that authorize the disclosure to third parties of information that is greater than necessary and that may prove damaging. Moreover, medical records may include information provided in confidence by family members, friends, and others that they would not want released to third parties.

Ideally, the psychiatrist who generated the original record would act as the guardian of the information it contains. Psychiatrists in solo private practice may be able to achieve this ideal. However, this may not be feasible in all settings, particularly those in which long-term relationships are not formed between psychiatrists and patients (e.g., emergency rooms). Moreover, psychiatric information may be embedded in the records of other physicians and controlled by them, as occurs when psychiatrists provide consultation or information to primary medical physicians. Nonetheless, it is important, for the reasons discussed, that psychiatrists—in concert with other physicians—continue to be the guardians of the record. One model for achieving this goal can be found in the traditional hospital where the medical staff is responsible for establishing policies for the medical record room and for supervising its operation. Thus, the medical staff can assure that implemented policies protect patient privacy, yet are practical and facilitate the appropriate flow of medical information. Often, hospital policies follow a graded approach. For example, in routine instances of disclosure, the release of medical information will not require the attention of treating psychiatrists (e.g., disclosure of billing information with the patient's consent). In other instances, the release of information may raise questions that require the exercise of medical judgment, but not necessarily that of the treating psychiatrist. Of course, in some cases the treating psychiatrist will need to be involved in the decision making process. Similar models of psychiatrist (and other physician) control of information must be implemented in new systems of health care.

B. Medical information should not be used for nonmedical purposes without appropriate authorization. As noted in the Guidelines, "The patient's consent to the release of in-

formation from his or her medical record should be informed and given freely, without threat or coercion." Moreover, "For their consent to be informed, patients should have an appreciation of the nature and content of the information to be released, the purposes for which it will be used, the manner in which it will be protected, and the extent to which any of the information may be redisclosed to other parties." Information disclosed for one purpose (e.g., to validate a claim for medical coverage) must not be used for another (e.g., to deny life insurance coverage). Insurers and recipients of disclosed information should be allowed to retain information for specified time-limited periods, in order to fulfill the stated purposes for which the information was released. Neither participation in an insurance plan nor access to private or governmental benefits should be contingent upon waiver of the general expectation of minimal, time-limited disclosure. Insurers should not be able to gather or accumulate medical data in order to deny health insurance to individuals.

C. New information technologies should not be employed to stretch the limits of appropriate access that have been established in professional custom and law. The role of psychiatrists in safeguarding patients' privacy includes protection from the scrutiny of law enforcement agencies. Courts have recognized the authority of physicians to object to law enforcement seizures of records on behalf of their patients who would otherwise be forced to forgo the privacy they seek to protect. Currently, procedural safeguards are in place to ensure that law enforcement agencies are seeking medical information for legitimate purposes and that the rights of patients are balanced against investigatory needs. Law enforcement agencies must seek judicial authorization to obtain access to records and, except in extreme circumstances, before a court order is granted, patients and responsible physicians (or their medical record room intermediaries) must be notified that records are being sought so that they have the opportunity to oppose the release of information. Law enforcement agencies bear the burden of proving in an adversarial hearing that the records contain information relevant to a legal inquiry.

The availability of electronic records has proved to be a substantial temptation to eliminate traditional privacy protections. In particular, oversight agencies and other law enforcement groups seek ready access to medical records in order to pursue criminal investigations of fraudulent billing practices. In other cases, law enforcement agencies may wish to scan hospital computer records in search of criminals. While the elimination of fraud and abuse and the apprehension of criminals are laudatory goals, traditional legal and professional safeguards should con-

tinue to protect patient privacy. When patients are targets of law enforcement inquiry, police agencies should not have access to records without patient consent, unless a court—following a full adversarial hearing—has concluded that the law enforcement interests outweigh the interests of the patient. When physicians are targets of law enforcement inquiry, judicial approval—but not an adversarial hearing, which would alert suspects who may destroy evidence—is necessary to ensure that there is cause to access the records. Regardless of whether physicians or patients are targets, an active role for the judiciary is critical for the preservation of privacy. *In camera* inspection of medical information will allow judges to determine whether law enforcement access is warranted. Moreover, in many cases, judges may be able to limit access to the record to nonidentifiable information (such as appointment and billing data). In other cases, judges will be able to limit access to redacted records that fulfill investigatory purposes, thus limiting the scope of the intrusion into patient privacy. For example, judges may redact detailed psychotherapy notes which contain the most private thoughts of patients that are rarely relevant to police investigations. Once they have gained access to information, law enforcement agencies should be bound to maintain the privacy of the records they obtain to the greatest extent possible. Moreover, when law enforcement agencies obtain medical records for purposes of investigating physicians, they must not be able to use these records against patients in any way.

3. Patients should have reasonable access to their records. Patients' right to access their own records has been recognized in many jurisdictions. Patients are the source of much of the data contained in records and may be able to identify inaccuracies or omissions. However, patients' access to their records should not be absolute. In some cases, patients may not be able to decipher their records without assistance. Psychiatrists may want to review the chart with the patient in order to clarify jargon, to interpret clinical impressions, and to respond questions and concerns that might arise. Moreover, in some instances, the psychiatrist will need to withhold information that may affect the mental or physical well-being of the patient or, alternatively, that may threaten the safety of others. In other instances, the psychiatrist may need to withhold information that has been given by family members, friends, or others on the condition that it remain confidential. New information technologies raise the possibility that patients may be able to access their records from remote locations, without the knowledge of their treating psychiatrists. Mechanisms and procedures must be implemented to allow psychiatrists to have the opportunity to oversee patient access to their records. As with disclosures to third parties, oversight by the treating psychiatrist is the ideal, but this may not be feasible in all practice settings for the reasons discussed earlier. However, it is necessary that psychiatrists—and other physicians—

control the information disclosure process to patients.

4. Researchers' access to medical records should continue to require respect for patient privacy. Over the last generation, a host of measures have been adopted to protect subjects of medical research. Medical records that are stored in an electronic form are easier to access and to manipulate than traditional records and, therefore, are likely to be sought out by researchers with increasing frequency in the future. The organizations that maintain these records must be responsible for providing oversight of research projects as Institutional Review Boards (IRBs) currently provide. When IRBs and other oversight bodies permit access to medical records in computerized form, they must limit access to only that information necessary to conduct the research. IRBs and oversight bodies should be alert to the potential of information technology as a means of enhancing privacy. For example, researchers who seek access to data contained in medical records typically do not need patients' names or other information that may be used to identify patients (e.g., address, phone numbers, social security numbers, zip codes). These identifiers should be stripped from computer records prior to allowing access. Moreover, researchers should not maintain identifying information in computerized or electronic forms without patient consent.
5. Legal and ethical sanctions for violations of patient privacy should keep pace with developments in technology. Professional organizations should continue to educate their members about the appropriate uses and the inherent risks of new information technologies. Patient privacy is fragile; once lost, it cannot be regained and its loss cannot be truly compensated. The best measures are ones that minimize the risk of inappropriate disclosure. As discussed above, the single, most effective measure is to maintain psychiatrists and physicians in their traditional role as guardians of the medical record. Professional organizations should continue to enforce vigorously ethical principles that require the confidentiality of patients' records to be maintained. Legal sanctions (breach of fiduciary duties, malpractice, breach of implied contract, etc.), when appropriate, should be applied for breach of confidentiality.

Appropriate legal sanctions need to be developed to cover insurers, industry, and other entities that have become increasingly important as recipients of health information. To date, these entities and their uses of medical information have been largely unregulated. Aggressive action—in accordance with the principles outlined here—is necessary if patient privacy is to continue to be protected in the coming era. One caveat should be noted. While federal legislation that encompasses new information practices and the various new entities in the health care arena may be necessary, care must be taken that the traditional protections found in the psychiatrist-patient relationship and existing state laws are not undermined.