Privacy in Psychiatric Treatment: Threats and Responses

Paul S. Appelbaum, M.D.

Objective: The author provides an overview of the current status of privacy in psychiatric treatment, with particular attention to the effects of new federal regulations authorized by the Health Insurance Portability and Accountability Act (HIPAA).

Method: The author reviews the ethical and legal underpinnings for medical privacy, including the empirical data supporting its importance; discusses those portions of the new federal regulations most relevant to psychiatric practice; and suggests steps that psychiatrists can take to maintain their patients' privacy in the new environment.

Results: Medical ethics and law, in keeping with patients' preferences, traditionally have provided strong protection for the information that patients communicate while receiving medical care. In general, release of information has required patients' explicit consent. However, limitations of the consent model and technological innovations that permit the aggregation of computerized medical information have led to pressure for greater access to these data. Although the new federal regulations offer patients some additional protections (including security for psychotherapy notes), they also mark a retreat from reliance on patient consent and open up records to previously unauthorized uses, among them law enforcement investigations and marketing and fundraising by health care organizations. However, states retain the power to provide higher levels of protection.

Conclusions: The new regulatory environment is less friendly to medical privacy but still leaves a great deal of discretion in physicians' hands. A commitment to protecting privacy as an ethical norm can be advanced by psychiatrists' requesting patients' consent even when it is not required, by ensuring that patients are aware of the limits on confidentiality, and by avoiding unnecessary breaches of privacy in the course of providing psychiatric care.

(Am J Psychiatry 2002; 159:1809–1818)

A long distance truck driver with a clean driving record is fired after his health insurance company informs his employer that he sought coverage—which the insurer denied—at an alcohol treatment clinic (1).

Newspaper accounts report that a health maintenance organization (HMO) with more than a million members has made computerized medical records of patients, including notes of psychotherapy sessions, available to all clinical personnel at every site (2). After the disclosure, psychotherapy notes are withdrawn from the computerized system.

A major university medical center discloses that thousands of patient records have been posted in error on its publicly available web site. Officials believe the records were available for 2 months before the mistake was discovered (3).

Privacy of communications between patients and physicians has long been a cornerstone of medical treatment. Since the Hippocratic Oath enjoined physicians not to tell of those things that "should not be published abroad" (4, p. 5), doctors and their patients generally have assumed that they could communicate in confidence the information necessary to conduct medical care. That has been particularly important in psychiatry, where the ability of patients to convey potentially embarrassing information is essential for accurate diagnosis and effective treatment. Although exceptions to the privacy of medical information have always existed, they were relatively circumscribed and seemed to reinforce, rather than undermine, the general rule.

In recent years, however, the assumption that medical information will remain a private matter between patients and physicians has been challenged by a series of changes in how medical records are kept and in the nature, oversight, and financing of medical practice. These changes include the formulation of a team approach to patient care (5), requirements for reporting behaviors such as child and elder abuse, aggressive government monitoring of care financed by public payers (6), demands by private insurers and managed care companies for access to patient records before authorizing payment (7), and the rapid computerization of medical record keeping, accompanied by the development of the Internet (8). Both the popular media and the professional literature evidence the resulting sense of unease about the potential loss of privacy of medical information (9, 10).

These concerns about the privacy of data generated in medical encounters, along with a growing recognition of the value of medical records for commercial, research, and governmental purposes, have combined to create a rapidly changing regulatory environment. Physicians and patients alike now face profound perturbations in the rules that have governed the disclosure of medical information. To clarify the current situation—with particular attention to psychiatric practice—this paper reviews the ethical and legal underpinnings of medical privacy and the sources of pressure for change, offers an overview of new federal regulations that are likely to alter profoundly many aspects of medical privacy, and provides suggestions to psychiatrists both for maintaining their patients' privacy in the new environment and for political and other initiatives that may mitigate the regulations' negative impact.

The Underpinnings of Medical Privacy

Privacy, as used in this discussion, is the interest that persons have in maintaining control of information about them; medical privacy refers specifically to information concerning persons' medical conditions. Confidentiality, a term that often is used interchangeably with privacy, refers more narrowly to the obligation to maintain privacy assumed by someone who enters into a relationship marked by the promise that information that is disclosed will not be revealed to others.

Ethical Underpinnings

What accounts for the long-standing tradition in medicine of protecting patients' privacy? Medical ethicists point to two deep-seated ethical rationales. The justification most commonly offered is a consequentialist or utilitarian one: if patients are to provide the information required for physicians to diagnose and treat them effectively, they must trust that their physicians will not disclose those data to third parties (11). In the absence of some guarantee of privacy, patients will either avoid coming for care, or if they do come, will withhold information necessary for treatment. This rationale seems particularly potent in psychiatry, where the information elicited from patients includes symptoms, behaviors, thoughts, and affects that might cause embarrassment, stigma, and discrimination were they to become generally known.

Consequentialist justifications can be susceptible, at least in principle, to empirical testing. Surveys of patients and of the population at large have confirmed that most people value highly the privacy of their medical information. For example, a recent Gallup survey conducted for the Institute for Health Freedom found that 78% of respondents felt that the confidentiality of their medical records was very important (12). As a corollary, there was strong opposition to giving nonmedical groups access to medical records. Thus, 95% of respondents opposed banks' having access to their records; 92% felt similarly about government agencies; 84% opposed access by the police, lawyers, or employers; and 82% opposed insurance companies' seeing their records without their consent. Studies of psychiatric (13, 14) and other mental health patients (15, 16) have revealed similar attitudes.

In keeping with utilitarian theory, those advocating a consequentialist basis for privacy must show that, in its absence, medical care would not be provided as effectively, i.e., that patients would withhold information from their caregivers or decline to come for treatment altogether. Although this argument seems self-evident to many privacy advocates, few attempts have been made to support this reasoning empirically, and the results have been mixed. A survey sponsored by the California Health Foundation revealed that 15% of a national sample reported doing something out of the ordinary to protect their medical privacy, including not seeking care and giving inaccurate or incomplete information (17). Probably the strongest data exist for adolescents, 25% of whom in one study said they would forego care if they thought their parents might find out (18). Another study of 2,224 high school students showed that those who perceived that their communications with physicians were confidential were more likely to have had pelvic exams and to have discussed sexual behavior and substance abuse with their doctors (19). On the other hand, 8% of respondents in that study reported that they actually had foregone care because of a fear that their parents would learn about their treatment.

Studies of mental health treatment have yielded mixed results, but often because the methods used were less than optimal. Some studies utilizing nonclinical samples (e.g., university students) found that varying the level of assurance of confidentiality did not affect the amount of information disclosed in an interview (20, 21), although other studies reached contrary conclusions (22). The relevance of these studies to real-life settings, however, is questionable. In the only two studies of this sort to examine patients currently receiving mental health treatment, when a variety of limitations on confidentiality were described, willingness to disclose and actual disclosure of information were reduced (23, 24). Overall then, although there are data suggesting that patients in mental health settings are similar to those in general health settings in the extent to which their disclosures may be negatively impacted by a lack of privacy, the number of studies is small and the data are not robust. Nonetheless, belief remains strong in the field that potential adverse effects on treatment constitute the strongest rationale for protection of patients' privacy.

Some students of medical privacy, however, impelled in part by the relative paucity of data supporting consequentialist justifications—especially in psychiatric treatment—have suggested that a second ethical argument be considered. They argue that medical privacy can better be justified by using what ethicists refer to as a deontologic approach, i.e., considering privacy as a good in itself, rather than seeing its value only in the positive effect it may have

on patients' health (25, 26). Most often, the role of privacy in advancing individual autonomy is identified as the basis for this claim. One commentator speaks of the "insulation that privacy provides so that as self-conscious beings we can maintain our self-respect, develop our self-esteem, and increase our ability to form a coherent identity and set of values, as well as our ability to form varied and complex relationships with others" (27, p. 213).

Although a deontologic argument for medical privacy can be applied to medical care in general, it probably works best for psychotherapy per se. The ability to speak freely with another person about one's innermost thoughts, fears, and passions is clearly dependent on the belief that one's revelations will go no farther. Creating a space within which this sort of dialogue can occur is likely to facilitate the conscious exploration of alternative modes of thought and behavior on which truly autonomous functioning rests. A society like ours, built on the premise that individual autonomy ought to be encouraged, should be receptive to the claim that protecting the privacy of the psychotherapeutic relationship carries positive social value. Indeed, insofar as psychiatrists deal largely with conditions that often impair autonomous function, the same argument might be advanced for psychiatric treatment in general.

The practical import of these ethical arguments is the widespread acceptance among members of the medical profession of the principle that physicians owe patients a duty of confidentiality, unless patients release them from it by offering consent for the disclosure of information. Embodied in the American Medical Association's *Principles of Medical Ethics* is the admonition that "[a] physician…shall safeguard patient confidences within the constraints of the law" (28, p. 2). The American College of Physicians, representing the nation's internists, is still more explicit: "To protect patient confidentiality, information should only be released with the written permission of the patient or the patient's legally authorized representative" (29). Similarly, the American Psychiatric Association's *Annotations* to the AMA's *Principles* holds that "[a] psychiatrist may release confidential information only with the authorization of the patient or under proper legal compulsion" (28, p. 6). The medical profession's ethical commitment to protecting privacy seems clear. However, since the boundaries of the profession's ethical duties appear to be circumscribed by the law, the parameters of legal protection for medical information assume particular significance.

Legal Underpinnings

Legal protection of medical privacy is a much more recent and fragmentary phenomenon than many people suppose. The law's first foray in this area was aimed at preventing the courts from compelling disclosure of information that physicians obtained in their attendance on patients. Abandoning the common law rule that the courts had the right to every person's testimony, New York in 1828 passed the nation's first statute establishing a physician-patient testimonial privilege. Under the privilege, patients had the right to prevent their physicians from testifying in regard to any information patients may have communicated in the course of treatment. In the century that followed, many states emulated New York, passing privilege statutes of their own (30). However, the courts were often hostile to medical privileges, since they were seen—not unreasonably—as complicating the adjudicatory process. Given that these privileges were usually defended on consequentialist grounds—i.e., as necessary to encourage patients to seek medical care—they were also susceptible to attack on the basis that patients with significant illnesses would pursue treatment regardless of whether a privilege existed, because patients typically did not need to communicate sensitive information to obtain medical care. By the mid-20th century, physician-patient privileges began to fall from favor, although they still exist in many jurisdictions.

As enthusiasm for physician-patient privileges declined in the second half of the 20th century, there was a concomitant rise in the number of states creating privileges designed specifically to cover mental health treatment, often denominated psychotherapist-patient privileges. Today, every jurisdiction in the United States offers some sort of privilege for treatment by mental health professionals, by no means limited to psychotherapy (31). Often riddled with exceptions (which may include, for example, testimony related to criminal offenses, child custody, and child abuse and testimony in cases in which patients have based a legal claim on some aspect of their mental state), these statutes nonetheless provide some real protection for patients. In 1996, the U.S. Supreme Court, exercising the discretion afforded it in the Federal Rules of Evidence, gave judicial recognition to a psychotherapist-patient privilege for the federal courts (31). The Court's decision in *Jaffee v. Redmond* offered strong support for privacy in psychotherapeutic treatment: "The psychotherapist privilege serves the public interest by facilitating the provision of appropriate treatment for individuals suffering the effects of a mental or emotional problem. The mental health of our citizenry, no less than its physical health, is a public good of transcendent importance" (31). Although the precise dimensions of the federal privilege will be determined by subsequent cases, it is worth emphasizing that it is likely to cover mental health treatment in general, rather than being limited to psychotherapy per se (32).

Parallel to the growth of privileges for treatment by mental health professionals has been the development of state statutes regulating the circumstances under which medical information can be disclosed to others besides the courts. These statutes create a patchwork of regulation, often focused on particular disorders, such as AIDS, or on diagnostic information, such as genetic testing (33). Forty-five states and the District of Columbia have statutes specifically addressing release of mental health information (34). Although their provisions vary greatly, many statutes address the criteria for a valid consent to release

of information, specify when information can be disclosed to other health professionals and to family members who may be involved in patients' care, and enumerate the circumstances under which access to data is allowed for other purposes, including research, public health needs, and quality improvement efforts (34).

While state legislatures were limiting the circumstances in which medical information can be disclosed without patients' consent, state courts were recognizing causes of action under which patients who were harmed by unauthorized disclosures could obtain appropriate compensation. A typical case, echoing decisions in other jurisdictions (e.g., references 35–37), is *Alberts v. Devine,* a 1985 decision of the Massachusetts Supreme Judicial Court (38). Alberts, a minister who had sought psychiatric treatment from Devine, lost his pulpit when the psychiatrist acquiesced in the request of Alberts's superiors and revealed the nature of his condition to them. The court held that patients have "a valid interest in preserving the confidentiality of medical facts communicated to a physician or discovered by the physician through examination." Hence, "a violation of that duty [of confidentiality], resulting in damages, gives rise to a cause of action sounding in tort against the physician" (35). Not only was Devine liable to compensate Alberts for the harm he suffered, but Alberts's superiors, who had induced Devine to violate his duty, were held liable as well. Like the other courts that have ruled in this area, the Massachusetts court recognized exceptions to the requirement of confidentiality when a danger existed to third parties or when disclosure was otherwise required by law.

To this point, the focus has been largely on state law and regulation, since until recently the federal government left regulation of medical privacy largely to the states. One important exception is embodied in the Public Health Service Act, which establishes special protections for the records of patients who receive treatment for alcohol or drug abuse in federally supported, specialty treatment programs (39). The resulting regulations strictly limit disclosure without the patient's consent to situations in which an emergency exists, a crime has been committed at the program, information has been obtained relating to child abuse, a court—applying a set of criteria that includes balancing the benefits and harms of disclosure—orders release, and a small number of other circumstances (40).

In sum, the impact of law on medical privacy by and large has been complementary to the thrust of the medical profession's ethical codes. Although there are a number of discrete exceptions, often involving a risk of harm to third parties (e.g., child abuse) or the superordinate needs of the courts, physicians have been obliged to respect patients' medical privacy. Patient consent has been the sine qua non required for disclosure of information, and physicians can be subject to civil actions, licensure proceedings, and, sometimes, criminal penalties for violation of that rule.

Pressure for Change

From where have the pressures come to alter these traditional approaches to the protection of patients' medical privacy? In part, there has been greater recognition in recent years of the limitations of the consent-based model. With medical care increasingly being rendered by large entities, rather than restricted to the physician-patient dyad, a growing number of caregivers and support staff gained access to patients' records. In 1982, internist Mark Siegler declared confidentiality "a decrepit concept," as he documented how as many as 100 people in his university hospital might have a legitimate need to examine a patient's medical record (5). During the intervening two decades, with outpatient care increasingly rendered in HMOs or large group practices, a similar effect has been seen for ambulatory care records. Since obtaining patients' consent each time someone other than their physicians accesses their records is impractical, many health care facilities have begun obtaining blanket consent for all staff to view patient records, or simply have assumed that patients acquiesced in staff members' having access, when that was necessary for their care. In these settings, the traditional model of consent for each disclosure fell by the wayside.

The number of people with access to patients' records was further magnified with the growth of third-party payers in the mid-20th century and the development of managed care in the late 1980s and 1990s. Tighter management of authorizations for payment, with the goal of holding down medical costs, often involves requests for large amounts of patient information—including entire medical records—as part of managed care companies' utilization review procedures (7). Although patients may be asked for consent, either at the inception of treatment or at the time the information is requested, they generally feel that they have no genuine choice about releasing information, since insurance coverage for their care is dependent on their agreement (41). Once the information is in the companies' hands, these entities are not bound by the traditional duties that have attached to physicians and, by extension, the facilities in which they deliver care. Thus, insurers and managed care companies have been free to transfer medical information to insurance industry databanks (42), pharmacy benefit management companies (43), or even patients' employers (44), without limits on further redisclosure.

At the same time that these developments were calling into question the efficacy of a consent-based approach, technological advances opened up new possibilities for the use of medical data. An influential 1991 report by the Institute of Medicine endorsed the adoption of computerized medical records as likely to improve the quality of care, advance medical science, lower health care costs, and enhance medical education (45). Just 3 years later, another Institute of Medicine panel enthusiastically sup-

ported the development of regional health data organizations that would aggregate medical information from all encounters of every patient, a process that would be greatly facilitated by computerized record systems (46). Among the uses that were envisioned for the resulting data were identifying patterns of illness and unmet needs; documenting inappropriate, wasteful, or harmful services; locating "cost-effective care providers"; and improving the quality of care—although the committee recognized that the very existence of easily accessible data of this sort would inevitably generate additional unanticipated requests for access. The Clinton administration's unsuccessful proposal for health care reform adopted this vision, embracing a national network of databases that would track every health care encounter (33).

If fully implemented, a web of computerized record systems feeding into a network of regional data banks would create what its proponents referred to as a "health information infrastructure" (10, 33). Large employers, insurers, hardware and software makers, law enforcement agencies, and researchers—each for their own reasons—lined up in support. Although the Clinton health proposal was defeated, the first steps toward establishing this infrastructure were taken in 1996, with the passage of the Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191). Among its provisions, the bill charged the Secretary of the Department of Health and Human Services (DHHS) with developing a "unique health identifier," a code that would allow each person's medical contacts to be aggregated from birth to death. Some such means of tracking individuals is an absolute requirement for the implementation of a system of regional or national data banks. (The Clinton administration imposed a moratorium on the development of a unique health identifier in August 1998, until medical privacy legislation was adopted; the HIPAA mandate, however, remains unchanged, and the process can be restarted at any time [44].)

Since many of the proponents of a health information infrastructure acknowledged that it would raise substantial concerns about medical privacy (33, 46), HIPAA required the Secretary of the Department of Health and Human Services (DHHS) to submit to Congress within 1 year "detailed recommendations on standards with respect to the privacy of individually identifiable health information."

The Secretary's report appeared in late 1997 (47). Recognizing that the traditional reliance on patient consent would make the goal of a databank network unattainable and pointing to the existing limitations of consent as a means of protecting patients' privacy, the Secretary recommended, "that the traditional control on use and disclosure of information, the patient's written authorization, be replaced by comprehensive statutory controls on all who get health information for health care and payment purposes" (47).

Under the DHHS proposal, patients would have lost control over release of their medical records, with the process governed instead by federal regulation. Congress, which had been trying for several years to pass privacy legislation, found itself caught between advocates of greater accessibility of medical records and privacy proponents. Recognizing that it was unlikely to break the logjam, Congress wrote into the HIPAA law a deadline of August 1999 for the passage of comprehensive medical privacy legislation. If the deadline was not met, DHHS would be empowered to draft binding regulations to accomplish what Congress could not. When Congress failed to pass a bill, DHHS issued draft regulations in late 1999 (48) and, after an extended comment period, published final regulations in December 2000, during the waning days of the Clinton administration (49). After a period of reconsideration, the regulations were formally promulgated by the Bush administration in April 2001 (50). Final changes, before implementation, appeared in August 2002 (51).

As the first effort to establish national standards for the privacy of medical information, these regulations (often referred to as the "HIPAA regulations" to denote their statutory lineage) are of immense significance. When they go into effect in April 2003, they will alter the way every physician deals with patient information and will affect the privacy rights of all persons who receive medical care. Moreover, far from codifying existing practice, the new rules will effect substantial changes in the handling of medical record information, limiting access without patient consent in a few areas, but broadening it beyond current bounds in a number of others. The regulations reflect the pressure that has been growing over the past decade to sacrifice individual control over medical data in favor of the purported social benefits of easier access to that information.

The New Federal Regulations

The privacy regulations themselves take up 31 pages of small print in the *Federal Register*; an accompanying official commentary occupies another 336 pages (49), with additional changes adding to the mass of detail (51). Rather than attempting to summarize this complex regulatory structure in its entirety, this section focuses on those elements of the regulations that are likely to be of greatest concern to psychiatrists. Broader summaries are beginning to appear (52), and interested readers are encouraged to review the regulations themselves in preparation for the changes they will bring.

Who must comply with the new rules? Under the terms of HIPAA, DHHS was authorized to write regulations that apply to health plans (e.g., insurers, HMOs, self-insurance programs), health care clearinghouses (i.e., entities that process health information), and health care providers who transmit any health information in electronic form. The latter is interpreted broadly to include submission of

claims, processing of bills, and transmission of other patient-related information. Indeed, even practitioners who do not use computers themselves, but who contract with billing services that transmit information electronically would be covered by the regulations (49, p. 82476). For now, it appears that clinicians who make no use of electronic transmission of data and contract with no other entities to do so on their behalf are exempt from the provisions of the HIPAA rules. As electronic submission of claims becomes routine, this group is likely to shrink considerably. Almost all the entities affected by the regulations (with the exception of small health plans, which have an extra year) have been given until April 14, 2003, to come into compliance with their terms.

Use and Release of Information for Treatment, Payment, and Health Care Operations

The rules governing use and release of individually identifiable information under the regulations differ according to the purposes for which the information is being used or disclosed. For those functions most closely related to the delivery of health care—denoted "treatment, payment and health care operations"—holders of health information need no longer obtain consent from their patients, though they can if they choose to (51, p. 53268). Instead, they are authorized by the regulations themselves to use and disclose the information, with few exceptions. Under these provisions, other caregivers, disease management companies, pharmacy benefit managers, utilization reviewers, quality improvement consultants, and many others will receive identifiable information without patient consent or knowledge. The regulations do require that covered entities make good-faith efforts to provide notice of their information policies to patients the first time service is rendered and to obtain patients' written acknowledgment. According to DHHS, this provision is designed in large part to offer patients an opportunity to ask questions about and discuss the information practices of those to whom they will be revealing health-related information. But the entities' ability to disclose such information is not dependent on patients' agreement; indeed, the regulations authorize such disclosure even over patients' specific objections.

This approach to use of health information, which negates the traditional reliance on patient consent, was initially proposed in DHHS Secretary Shalala's report in 1997 (47) and was reflected in the draft regulations issued by the Clinton Administration in 1999 (48). But when the final version of the Clinton regulations appeared at the end of 2000, they embodied an alternative approach that asked patients to provide blanket written consent for use and release of their medical information at the time of enrollment into a health plan or the inception of treatment (49, p. 82810). The Bush Administration's decision to reject patient consent as the basis for disclosure of information was premised in part on the assertion that the Clinton consent requirement provided little meaningful protection for patients in any event. Clearly, the Administration was also responding to objections from the health care, pharmacy, and insurance industries, among others, about the cost and inconvenience associated with reliance on written consent. Thus was lost the historic right of patients to control dissemination of their medical records. This represents the most profound change in traditional practices wrought by the HIPAA regulations.

Use and Release of Information for Other Purposes Requiring Authorization

Except for treatment, payment, health care operations, and the special categories described in the following section, all other uses of identifiable health information require something that the regulations refer to as the patient's "authorization" but that resembles consent as most physicians and facilities are familiar with the term (51, p. 53268). The authorization forms must indicate the information to be used or disclosed, the purposes to which it will be put, and the recipient of the information, and they must contain an expiration date. Thus, for example, for information to be disclosed to a patient's employer for use in a hiring or promotion decision, the patient must provide this kind of written authorization. For non-health-care uses that are not addressed specially elsewhere in the regulations, this provision offers real protection for patients' privacy.

Use and Release That Does Not Require Consent or Authorization

Twelve uses are identified specially as justifying the release of identifiable health information without patients' consent or authorization, and generally without their even being told that disclosure has occurred. Some of these uses of information are familiar to clinicians and consistent with current practice, for example, "to avert a serious threat to health or safety" (49, p. 82817) or to report child abuse or neglect (49, p. 82814). Other provisions are more problematic. Thus, during litigation, health information can be released in response to a request for discovery or a subpoena from an attorney—even one representing a party adverse to the patient—as long as the attorney provides assurance that reasonable efforts have been made to notify the patient of the request (49, p. 82814). The absence of a requirement for judicial review of these requests means that, unless patients respond quickly enough to block disclosure, attorneys will be able to obtain medical records of parties to the case and conceivably of their witnesses as well.

Law enforcement lobbied heavily during the process of drafting these regulations for greater access to medical records. In the final version, police officers can be given access to records on the basis of an administrative request, without judicial review (49, p. 82815). Disclosure of identifying information and some details of patients' treatment can occur in response to a simple inquiry from a law enforcement officer for the purposes of "identifying or locat-

ing a suspect, fugitive, material witness or missing person." If the police desired to enter a person's house to examine their possessions for any of these reasons, they would be required to obtain a search warrant from a magistrate and to demonstrate probable cause that the search will discover information related to the crime. However, under the HIPAA regulations, police can search medical records without ever having to step before a judge to demonstrate the reasonableness of their request. Separate provisions permit disclosure to national security agencies and the Secret Service that go well beyond current practices; the Secret Service, for example, has gone to great lengths to train its agents to work within the limits imposed by state law and requirements for patient consent (53), but the regulations would free them of that burden.

Fundraising also constitutes an exception to the usual requirements for consent or authorization (49, p. 82820). Holders of health information can disclose to other entities that are assisting them in raising funds the identity of their patients, demographic information, and the dates that health care was provided. This can be particularly problematic for patients treated in psychiatric or other specialized facilities, where identification of the locus of treatment indicates the nature of the patient's condition. A similar exemption exists for disclosure of information for the purpose of marketing services delivered by the facility that originally treated the patient (49, p. 82819). A set of complex rules governs marketing by health care providers and health plans, requiring authorization if information is being sold for marketing purposes, but allowing information to be used for many forms of marketing by the information holders themselves and their business associates (51, p. 53267).

Access to medical records for research purposes was a contentious issue as the regulations were being formulated. Researchers, particularly those using existing data bases, objected to the possibility of being required to obtain consent from every person whose data they wished to access (54, 55). In response, DHHS allowed the requirement for authorization for research use to be waived by an Institutional Review Board constituted according to the federal Common Rule that governs most research in this country, or by a privacy board set up specifically for the purpose (49, p. 82816; 51, p. 53270). The criteria largely reflect current practices, including a demonstration that the research presents no more than a minimal risk to subjects and could not be practicably carried out without the waiver. This represents a reasonable accommodation of the interests of both researchers and patients (56).

Use and Release of Psychotherapy Notes

Of particular interest to psychiatrists, psychotherapy notes have been given protections by these regulations that were not afforded to any other medical records (49, p. 82811). Psychotherapy notes cannot be released, with a small number of exceptions, without the explicit authorization of the patient. Moreover, neither treatment nor payment by insurers can be conditioned on release of psychotherapy notes. This provision reflects a recognition by DHHS that the information contained in psychotherapy notes is likely to be qualitatively different from that found elsewhere in the medical record. In the preamble to the regulations, DHHS specifically cites the rationale of the U.S. Supreme Court's decision in *Jaffee v. Redmond* (31) as motivating its treatment of this issue.

Although these extra safeguards for psychotherapy notes will be welcomed by most therapists, they are not quite as sweeping as they seem at first blush. In order to qualify for this protection, the notes in question must be kept separate from the patient's medical record, requiring a second chart in many cases. Excluded from protection are information about medication prescription and monitoring, start and stop times, modalities and frequencies of treatment furnished, results of clinical tests, and summaries of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date. Thus, a great deal of sensitive information—for example, most of the information routinely collected during an intake evaluation—that would ordinarily be protected under a psychotherapist-patient privilege such as *Jaffee*'s, will not qualify for protection under this provision. A more effective means of protecting sensitive psychiatric information would have been to extend the protections now afforded to psychotherapy notes to the entire record of psychiatric treatment.

Other Provisions of the Regulations

There are several other aspects of the regulations of which clinicians should be aware. Patients are granted fairly sweeping rights to have access to and obtain a copy of their medical records, except for psychotherapy notes. Only a small number of exceptions to this general rule exist, the most significant of them being when "the access requested is reasonably likely to endanger the life or physical safety of the individual or another person" (49, p. 82823). If patients believe that the information in their record is inaccurate, they will have the right to request an amendment to the record. Denials of these requests must be justified in writing, and patients must be given the opportunity to submit a statement of disagreement, which becomes part of their medical record. Some states already have patient access provisions similar to these, but this will be new to much of the country and will create a uniform national standard of practice.

As a general rule, when releasing information from a patient's record, reasonable effort must be made "to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request" (49, p. 82805). The primary exception to this rule is when disclosure is being made to a health care provider for purposes related to treatment. When a request for information is made by another entity covered by the regulations, holders of medical records will be permitted to rely

on the requester's judgment that the latter has asked for the minimum necessary amount of information (57).

Along with learning the new rules for disclosure of medical record information, clinicians will have to meet a number of administrative requirements. Each "provider"—even a single physician's office—will need to develop formal privacy policies and procedures and designate a staff person as a "privacy official" who will receive complaints from and provide information to patients (49, p. 82826). All staff members must be trained in these policies, and, as noted, new patients will need to be provided with a notice of the relevant privacy practices. Patients have the right to receive an accounting of all disclosures from their medical records in the past 6 years, except for those made for treatment, payment, and health care operations, those they themselves have authorized, and a small number of other categories. Every provider will need to create and sign contracts with all business associates who are given access to identifiable information about patients (e.g., billing and transcription services, accountants, etc.) binding them to observe the terms of the regulations—to which, under the terms of HIPAA itself, they would not otherwise be subject. Medical societies have expressed considerable concern about the costs of implementing these provisions, especially for solo practitioners and small practices. General medical and specialty groups—including the American Medical Association and the American Psychiatric Association—have begun producing detailed guides for their members that provide advice on applying the regulations to their own practices.

Given that extensive state law and regulation already exist in this area, a final important consideration is how the federal regulations relate to these rules. As a general matter, the HIPAA regulations preempt state laws that are less protective of patients' privacy, creating a uniform floor of protection throughout the country (49, p. 82801). States retain the authority, however, to enforce a higher level of privacy protection, which means that practitioners will need to be aware of both the laws in their own jurisdictions and the federal rules. Other state laws that are not preempted by the regulations include those requiring reporting of events of public health significance, such as child abuse or communicable diseases, and laws relating to controlled substances. A procedure has been established for the Secretary of DHHS to determine whether a state law is more or less protective of privacy—something that may not always be clear, for example, when the same statute is more protective in one area and less in another.

Evolution of the Regulations

Although it appears at this point that the general form of the regulations will be retained for the indefinite future, there are likely to be some changes in specifics. DHHS has indicated that it will issue a set of guidance documents clarifying some aspects of the regulations and responding to frequently asked questions; the first of those advisories has already appeared (57). In addition, DHHS has the power to seek additional changes in the regulations, through its formal rule-making process, on a yearly basis.

More frontal assaults on the regulations have already begun. Two state medical societies have filed a lawsuit seeking to block implementation of the regulations, primarily on the grounds that Congress acted unconstitutionally in delegating power to DHHS to fashion these rules, without providing sufficient guidance (58). There are also rumblings from various congressional sources regarding legislation that would delay implementation or replace the regulations with statutory guidelines. However, since DHHS was empowered to enact these regulations only after years of failure by Congress to pass just such a bill, it seems unlikely that Congress will step back into this thicket.

Protecting Patient Privacy Under the HIPAA Regulations

What is the future of patient privacy in psychiatric treatment? The HIPAA regulations, although they take some positive steps toward greater privacy protection—limiting sale of medical information and providing greater security for psychotherapy notes, for example—fall far short of an optimal balancing of patients' interests with demands for access to patient-identifiable data. When the regulations go into effect in 2003, consent will no longer be required for disclosures related to treatment, payment, and health care operations. New avenues for access to medical information have been created (e.g., for law enforcement), while gaps in current protections have been addressed only in part (e.g., disclosures for purposes of marketing) or not at all. As an example of an area neglected by the regulations, no overt limits are set on the excessive demands of managed care companies for patient records in their utilization review process (although it is possible that the provision described earlier for the "minimum necessary" disclosure may be helpful over the long run here).

Despite the sweeping nature of these regulations, it is important to reflect on the ways in which greater privacy protections can be made available to patients. Perhaps most crucial is the fact that the HIPAA regulations do not override state laws that are more protective of medical privacy. Thus, in states that have case law, statutes, or regulations mandating, for example, patient consent before the release of medical information, those rules will take precedence over the less stringent federal regulations. States without such rules will retain the opportunity to adopt new laws restricting access to medical data. The insurance and managed care industries and representatives of large corporations can be expected to continue lobbying Congress to revoke HIPAA's nonpreemption provision, so as to impose a uniform set of federal regulations on the nation as a whole. For now, however, more protective state laws take precedence. Patients, clinicians, and professional as-

sociations desiring greater privacy safeguards are likely to direct their efforts toward their state houses.

Moreover, the regulations, which generally permit but do not require disclosure in the various circumstances they address, leave a great deal of discretion in the hands of health care professionals and facilities. Practitioners, clinics, and hospitals are not precluded from creating policies of their own that are more protective than the federal rules, so long as the data are stored locally. They might, for example, require informed consent before each disclosure of information, except for routine billing data. Although the regulations do not require holders of medical information to agree to limits on disclosure that are requested by patients, clinicians retain the discretion to do so. Thus, patients who are particularly concerned that their psychiatric record not be disseminated beyond their psychiatrist's office can negotiate specific limits that, once agreed to, would be binding on the psychiatrist. Even demands for information by attorneys, law enforcement, and other entities authorized under the HIPAA regulations to make such requests need not be acceded to by clinicians without patient consent, unless required by some other law.

An additional safeguard that clinicians can employ is to discuss with patients at the inception of treatment the limits on confidentiality of disclosed information. The new federal regulations, as noted, require that patients be informed in writing of a practitioner's or facility's privacy policies, but those documents may turn out to be insufficiently informative for many patients. A clear description of the foreseeable risks to privacy that might be material to a patient's decision to disclose sensitive information and a willingness to discuss ways of protecting privacy (e.g., omitting certain information from the record, or limiting it to a separate set of psychotherapy notes) could go a long way toward helping patients understand the privacy risks they face. Data from several studies suggest that information about limits to confidentiality is already the information that therapists reveal most frequently to patients at the start of treatment (59–62), although by no means do all patients receive such information (63, 64).

Nor can clinicians afford to ignore their behavior outside the realms directly governed by the HIPAA regulations and state law. Reports of discussions about patients in public elevators (65) or of psychiatric records being discarded in a dumpster when a practice is closed (66) point out how greatly patients' privacy rests in their physicians' hands. Complicated dilemmas relating to patients' privacy will only grow as the use of information technology proliferates (67) and as new medical techniques such as genetic profiling become common (68). Already clinicians must attend to protecting privacy when using web sites, e-mail, cell phones, voice mail, faxes, and other communications technology (69). In the long run, psychiatrists' dedication to the ethical principles underlying medical privacy will remain one of the most important protections that can be offered to patients.

Received Sept. 4, 2001, revision received Jan. 16, 2002, accepted Feb. 4, 2002. (Further revisions were made in August 2002, after changes in the federal regulations authorized by HIPAA were issued.)
From the Department of Psychiatry, University of Massachusetts Medical School. Address correspondence to Dr. Appelbaum, Department of Psychiatry, University of Massachusetts Medical School, Worcester, MA 01655; appelbap@ummhc.org (e-mail).

References

1. Goldstein A: Long reach into patients' privacy: new uses of data illustrate potential benefits, hazards. Washington Post, Aug 23, 1999, p A1
2. Bass A: HMO puts confidential records on-line: critics say computer file-keeping breaches privacy of mental health patients. Boston Globe, March 7, 1995, p 1
3. Upton J: Michigan medical records accidentally posted on Web. Detroit Free Press, Feb 12, 1999
4. Resier SJ, Dyck AJ, Curran WJ: Ethics in Medicine: Historical Perspectives and Contemporary Concerns. Cambridge, Mass, MIT Press, 1977
5. Siegler M: Confidentiality in medicine: a decrepit concept. N Engl J Med 1982; 307:1518–1521
6. Questions raised about Medicaid investigators. Psychiatr News, Nov 17, 1989, p 17
7. Corcoran K, Winslade WJ: Eavesdropping on the 50-minute hour: managed mental health care and confidentiality. Behav Sci Law 1994; 12:351–365
8. US Congress, Office of Technology Assessment: Protecting Privacy in Computerized Medical Information, OTA-TCT-576. Washington, DC, US Government Printing Office, Sept 1993
9. Appleby J: File safe? health records may not be confidential. USA Today, March 23, 2000, p 1
10. Appelbaum PS: A "health information infrastructure" and the threat to confidentiality of health records. Psychiatr Serv 1998; 49:27–28, 33
11. Gillon R: Philosophical medical ethics: confidentiality. Br Med J 1985; 291:1634–1636
12. Public Attitudes Toward Medical Privacy. Submitted to the Institute for Health Freedom. Princeton, NJ, The Gallup Organization, Sept 2000. www.forhealthfreedom.org/Gallupsurvey/IHF-Gallup.html
13. Schmid D, Appelbaum PS, Roth LH, Lidz CW: Confidentiality in psychiatry: a study of the patient's view. Hosp Community Psychiatry 1983; 34:353–355
14. Appelbaum PS, Kapen G, Walters B, Lidz CW, Roth LH: Confidentiality: an empirical test of the utilitarian perspective. Bull Am Acad Psychiatry Law 1984; 12:109–116
15. McGuire JM, Toal P, Blau B: The adult client's conception of confidentiality in the therapeutic relationship. Prof Psychol Res Pr 1985; 16:375–384
16. VandeCreek L, Miars R, Herzog CE: Client anticipations and preferences for confidentiality of records. J Counsel Psychol 1987; 34:62–67
17. Medical Privacy and Confidentiality Survey. Oakland, Calif, California Health Foundation, Jan 28, 1999. http://admin.chcf.org/documents/chcf/survey.pdf
18. Cheng TL, Savageau JA, Sattler AL, DeWitt TG: Confidentiality in health care: a survey of knowledge, perceptions, and attitudes among high school students. JAMA 1993; 269:1404–1407
19. Thrall JS, McCloskey L, Ettner SL, Rothman E, Tighe JE, Emans SJ: Confidentiality and adolescents' use of providers for health information and for pelvic examinations. Arch Pediatr Adolesc Med 2000; 154:885–892

20. McGuire J, Graves S, Blau B: Depth of self-disclosure as a function of assured confidentiality and videotape recording. J Couns Dev 1985; 64:259–263
21. Muehleman T, Pickens BK, Robinson F: Informing clients about the limits to confidentiality, risks and their rights: is self-disclosure inhibited? Prof Psychol Res Pr 1985; 16:385–397
22. Nowell D, Spruill J: If it's not absolutely confidential, will information be disclosed? Prof Psychol Res Pr 1993; 24:367–369
23. Kremer TG, Gesten EL: Confidentiality limits of managed care and clients' willingness to self-disclose. Prof Psychol Res Pr 1998; 29:553–558
24. Taube DO, Elwork A: Researching the effects of confidentiality law on patients' self-disclosures. Prof Psychol Res Pr 1990; 21: 72–75
25. Shuman DW, Weiner MF, Pinard G: The privilege study, part III: psychotherapist-patient communications in Canada. Int J Law Psychiatry 1986; 9:393–429
26. Imwinkelried E: The rivalry between truth and privilege: the weakness of the Supreme Court's instrumental reasoning in *Jaffee v Redmond,* 518 US 1 (1996). Hastings Law J 1998; 49: 969–990
27. DeCew JW: The priority of privacy for medical information. Soc Philosophy and Policy 2000; 17:213–234
28. American Psychiatric Association: The Principles of Medical Ethics With Annotations Especially Applicable to Psychiatry. Washington, DC, APA, 1998
29. American College of Physicians: Ethics manual. Ann Intern Med 1998; 128:576–594
30. Shuman DW: The origins of the physician-patient privilege and professional secret. Southwestern Law J 1985; 39:661–687
31. Jaffee v Redmond, 518 US 1 (1996)
32. Finley v Johnson Oil Company, 199 FRD 301, 2001 US Dist Lexis 1645 (SD Ind, Jan 18, 2001)
33. Gostin LO: Health information privacy. Cornell Law Rev 1995; 80:451–528
34. Petrila J: Legal and ethical issues in protecting the privacy of behavioral health care information (with appendix on state mental health law confidentiality provisions), in Privacy and Confidentiality in Mental Health Care. Edited by Gates JJ, Arons BS. Baltimore, Paul H Brookes, 2000, pp 91–125, 219–232
35. Horne v Patton, 291 Ala. 701 (1974)
36. MacDonald v Clinger, 84 A 2d 482 (NY 1982)
37. Hague v Williams, 37 NJ 328 (1962)
38. Alberts v Devine, 479 NE 2d 113 (Mass 1985)
39. 42 United States Code, Section 290dd-2
40. Samuels PN: Confidentiality of alcohol and other drug patient records, in Privacy and Confidentiality in Mental Health Care. Edited by Gates JJ, Arons BS. Baltimore, Paul H Brookes, 2000, pp 173–192
41. Kinzie, JD, Holmes JL, Arent J: Patients' release of medical records: involuntary, uninformed consent? Hosp Community Psychiatry 1985; 36:843–847
42. Garfinkel S: Database Nation: The Death of Privacy in the 21st Century. Sebastopol, Calif, O'Reilly & Associates, 2000
43. Lo B, Alpers A: Uses and abuses of prescription drug information in pharmacy benefit management programs. JAMA 2000; 283:801–806
44. Scarf M: The privacy threat that didn't go away: brave new world. New Republic, July 12, 1999, pp 16–18
45. Dick RS, Steen EB (eds): The Computer-Based Patient Record: An Essential Technology for Health Care. Washington, DC, National Academy Press, 1991
46. Donaldson MS, Lohr KN (eds): Health Data in the Information Age: Use, Disclosure, and Privacy. Washington, DC, National Academy Press, 1994
47. Confidentiality of Individually Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, Pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996. Washington, DC, Office of the Secretary, US Department of Health and Human Services, Sept 11, 1997. http://aspe.hhs.gov/admnsimp/pvcrec0.htm
48. Office of the Secretary, Department of Health and Human Services: Standards for privacy of individually identifiable health information. Federal Register 1999; 64:59918–60065
49. Office of the Secretary, Department of Health and Human Services: Standards for privacy of individually identifiable health information; final rule. Federal Register 2000; 65:82462–82829 (www.hhs.gov/ocr/hipaa)
50. Office of the Secretary, Department of Health and Human Services: Standards for privacy of individually identifiable health information. Federal Register 2001; 66:12434
51. Office of the Secretary, Department of Health and Human Services: Standards for privacy of individually identifiable health information. Federal Register 2002; 67:53182–53273
52. Gostin LO: National health information privacy: regulations under the Health Insurance Portability and Accountability Act. JAMA 2001; 285:3015–3021
53. Disclosure of Mental Health Information: A Secret Service Guide to Applicable State Law. Washington, DC, US Secret Service, Department of the Treasury, 1997
54. Melton LJ III: The threat to medical-records research. N Engl J Med 1997; 337:1466–1470
55. Simon GE, Unützer J, Young BE, Pincus HA: Large medical databases, population-based research, and patient confidentiality. Am J Psychiatry 2000; 157:1731–1737
56. Appelbaum PS: Protecting privacy while facilitating research (editorial). Am J Psychiatry 2000; 157:1725–1726
57. Standards for Privacy of Individually Identifiable Information. Washington, DC, Office for Civil Rights, Department of Health and Human Services, 2001. http://www.hhs.gov/ocr/hipaa/finalmaster.html
58. Landa AS: HHS sued over medical privacy rules. Am Med News, Aug 6, 2001, pp 5, 7
59. Talbert FS, Pipes RB: Informed consent for psychotherapy: content analysis of selected forms. Prof Psychol Res Pr 1988; 19: 131–132
60. Beeman DG, Scott NA: Therapists' attitudes toward psychotherapy informed consent with adolescents. Prof Psychol Res Pr 1991; 22:230–234
61. Somberg DR, Stone GL, Claiborn CD: Informed consent: therapists' beliefs and practices. Prof Psychol Res Pr 1993; 24:153–159
62. Jensen JA, McNamara JR: Parents' and clinicians' attitudes toward the risks and benefits of child psychotherapy: a study of informed-consent content. Prof Psychol Res Pr 1991; 22:161–170
63. Baird KA, Rupert PA: Clinical management of confidentiality: a survey of psychologists in seven states. Prof Psychol Res Pr 1987; 18:347–352
64. Nicolai KM, Scott NA: Provision of confidentiality information and its relation to child abuse reporting. Prof Psychol Res Pr 1994; 25:154–160
65. Ubel PA, Zell MM, Miller DJ, Fischer GS, Peters-Stefani D, Arnold RM: Elevator talk: observational study of inappropriate comments in a public space. Am J Med 1995; 99:190–194
66. Schwartz J: When public goes private: why were psychiatric files blowing down our street? Washington Post, Dec 22, 1996, p C1
67. Hodge JG, Gostin LO, Jacobson PD: Legal issues concerning electronic health information: privacy, quality, and liability. JAMA 1999; 282:1466–1471
68. Laurie GT: Challenging medical-legal norms: the role of autonomy, confidentiality, and privacy in protecting individual and familial group rights in genetic information. J Legal Med 2001; 22:1–54
69. Gutheil TG, Appelbaum PS: Clinical Handbook of Psychiatry and the Law, 3rd ed. Philadelphia, Lippincott Williams & Wilkins, 2000